MAAWG

December 8th, 2011

The Honorable Patrick Leahy
U.S. Senate
Chairman, Committee on the Judiciary
224 Dirksen Senate Office Building
Washington, DC 20510
Via Fax direct to committee: 1-202-224-9516

The Honorable Lamar Smith
U.S. House of Representatives
Chairman, Committee on the Judiciary
2138 Rayburn House Office Building
Washington, DC 20515-6216
Via email to committee clerk: olivia.lee@mail.house.gov

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 Chairmen Leahy and Smith:

The Messaging Anti-Abuse Working Group (MAAWG) is an international nonprofit organization founded to fight online abuse such as phishing, botnets, fraud, spam, viruses and denial-of-service attacks that can cause great harm to both individuals and national economies. MAAWG draws technical experts, researchers and policy specialists from a broad base of Internet service providers (ISPs) and network operators representing over one billion email accounts, and from key technology providers, academia, and volume messaging sender organizations. The multi-disciplinary approach at MAAWG includes education, advice on public policy and legislation, development of industry best practices and standards, and the facilitation of global collaboration.

MAAWG is first and foremost a technical organization, rather than a lobbying organization, and we have been successful in helping our members, and the Internet community as a whole, develop defenses against botnets, phishing, spam and online fraud. Recently it has come to our attention that Congress is considering legislation that would require the filtering of Internet Protocol ("IP") addresses, domains, sub domains and/or sub-directories for the purposes of combating online copyright infringement. While MAAWG is supportive of appropriate efforts to resolve the legitimate issues facing the intellectual property community, MAAWG members share a growing sense of concern with respect to the proposed use of these filtering techniques because we believe this solution will cause unintended harm. We are writing you today to express some of those concerns and offer the technical observations below.

Summary: Based upon decades of cumulative Internet industry experience, MAAWG has grave concerns that the technologies outlined in these bills will, in fact, *not* achieve the stated objectives. While some filtering techniques have been used in the past for cybersecurity purposes, in our experience cybercriminals have proven to be adept at exploiting or evading DNS and IP address filtering for many years and can readily avoid detection and "game" the system with little effort or cost.

On the other hand, it is critical to note that the deployment of these technologies would unintentionally increase security risks to end users and create new cyber attack targets that could possibly endanger public welfare. The filtering technologies outlined in these bills also would significantly impact the currently reliable messaging processes that are depended on worldwide and would require drastic architectural changes to existing network operations. These bills, if passed in their present form, will make it exceedingly difficult – if not arguably impossible – to protect the Internet community from ongoing attacks on critical infrastructure, to block spam, child pornography and malware, and to prevent phishing attacks against individuals and commercial enterprises.

We further note the adverse behavioral affect these techniques will promote by providing incentives to those end users who still want to access this illicit content by circumventing existing controls and to those sites distributing infringing content who will employ techniques similar to those used by cybercriminals. Causing basic infringers to "step up their game" will only make it harder to detect, identify and prosecute or litigate their behaviors. If you indirectly drive users in these extreme directions, existing investigative methods will only work against the most unsophisticated infringers.

There are those who dismiss such concerns as esoteric technical issues only on the minds of a few engineers or of those who wish to change current copyright régimes. Nothing could be further from the truth. What follows are technical explanations of real-world criticisms regarding the measures you are considering, initiatives that will render current online protection measures useless. The practical consequences to the public and to international commerce by the implementation of these bills as they are currently written could not be more dire.

Explanation: With respect to the requirement to filter Internet Protocol addresses, domains, sub domains, and/or sub-directories, we offer the following detailed observations:

1. DNS filtering will make – at best – a limited contribution to the accomplishment of the Acts' goals while conveying very disconcerting risks to network security, stability, and performance. Copyright infringers and other cybercriminals can, and will, create technical alternatives to operator-run Domain Name Servers under the Acts' proposed technical controls and they will be able to register new domain names, at negligible cost and in mere minutes, turning the Acts' efforts to block their websites into nothing more than a trivial nuisance.

   This has been proven over the years by the experience of the private sector. For the last decade, various technologies have been deployed within the private sector to limit or block the DNS resolution of illicit domain names in an effort to combat cybercrime. All the techniques in use, or that have been proposed, have known flaws that professional cybercriminals and copyright infringers could exploit to readily evade detection (for example, Domain-fluxing). Commercial services provided by Dynamic DNS (DDNS) operators often provide "domain tasting" or "free domain name" registration services that can enable cybercriminals or copyright infringers to rapidly hop from one domain name to the next. Research has shown that statically compiled blacklists, which are the traditional method of regulating DNS filtering, remain many weeks behind the initial assignment period during which the domain names are used for criminal purposes[1].

   It is also very likely that a segment of end users will continue to try to access the infringing content, regardless of any filtering efforts. Consequently, if this legislation results in a significant increase in DNS filtering it will also potentially create an incentive for users to evade DNS filters, especially since this can be easily done.

2. The alternative mechanisms that would be used to circumvent the controls in the Act can cause substantial collateral damage to law-abiding Internet users, merchants, government, and ISPs, and will expose legitimate Internet users to greater security issues. The range of threats to end users, networks, and organizations includes domain theft, spoofing, denial-of-service attacks, botnets, phishing, fraud, identity theft, and financial theft.

   Regardless of whether domain names are blocked at the edge level, a straightforward alternative that copyright infringers would likely employ is to simply alter the default recursive DNS server settings of the end users device that would like to access sites with illegal materials. Recent examples of this in terms of security are the "DNSChanger" bot network[2] and rogue DNS redirection in Brazil.

If copyright infringers adopted such a tactic extensively, network operators and security personnel would find themselves in an increasingly untenable position as an "alternative" Internet ecosystem is constructed. End users impacted by this change would be routed through an alternative recursive DNS infrastructure. Cybercriminals could take advantage of this situation to distribute malware and route DNS resolutions from the infected devices through the criminals' infrastructure and subvert the communications for their own gain. For example, cybercriminals could launch man-in-the-middle attacks that intercept and decrypt encrypted communications. The research community has extensively studied the "DNS Poisoning" activities that would be required for enforcement of the Act[3,4].

Further, as cybersecurity is a shared responsibility, one infected machine can impact many others. Consequently, the damage will not be limited to only those individuals seeking infringing content but could potentially have a multiplying effect.

3. DNS redirection or filtering from an offending site to another site or Web page – even if that page simply contains text indicating it is a "rogue site" and therefore not accessible – is inconsistent with the design of other critically needed Internet security technologies such as the DNS security extensions, or what is referred to as DNSSEC. There are several security challenges threatening the DNS infrastructure today. One type is DNS cache poisoning which involves tricking a DNS server to cache false information; for example, associating a domain with an incorrect IP address that directs end users to a fraudulent website used to facilitate identity theft or other malicious activities. This type of attack is of concern to the Internet security community and DNSSEC was developed, starting as far back as the late 1990s, to add an element of validation to DNS requests to ensure the results returned to an end user are, in fact, the actual IP address associated with the requested site. The DNSSEC standard was completed by the Internet Engineering Task Force (IETF) in 2005 and the root zone was signed by the U.S. Department of Commerce, the Internet Corporation for Assigned Names and Numbers (ICANN) and Verisign in 2010.

   The proposed DNS response suppression and/or redirection are technically indistinguishable from DNS cache poisoning by cybercriminals. Given that MAAWG and its members have been working to promote and deploy DNSSEC, as urged by the Department of Homeland Security and other agencies in the Executive Branch, and that networks, businesses, and users will soon start to rely upon DNSSEC for their security, Web browsing, e-commerce, and communications needs, we have concerns with legislation proposing measures incompatible with and undermining such key Internet security enhancements.

4. If DNSSEC is in operation when attempts are made to hijack, block or "poison" a DNS resolution, non-properly crafted answers will be passed to the end devices that issued the resolution request, possibly overwhelming system resources. DNSSEC responses contain cryptographically verifiable content to ensure the integrity of the communications. If it is not possible to verify the integrity of the DNSSEC response, recursive DNS servers and end devices are expected to ignore or distrust the response and even retry the request. There is a computational and resource cost to verifying the integrity of every DNSSEC resolution. It is clear that the cascade affect of a rejection/retry process will cause major problems to the recursive DNS servers operated around the world as it would exponentially increase memory and CPU utilization, possibly causing them to eventually fail or requiring additional infrastructure to maintain the current level of performance.

5. Sustained, centralized lists of domain names to be filtered as part of the alerting protocol of SOPA creates a new and significant attack target and vector for hackers, criminals, and hostile foreign states engaged in cyber-warfare and espionage. Hacking into these centralized filter lists and adding a legitimate domain name to the list could create a denial-of-existence attack, which would deny service to a legitimate site for potentially tens of millions of users in one stroke. One can imagine the chaos that could result by denying the existence of irs.gov on tax day; senate.gov on election day; amazon.com on cyber-Monday; or email, instant messaging, or Voice Over IP (VoIP) domains in the event of a national emergency or major natural disaster.

The agile nature of known “flux-based” evasion techniques poses additional problems for static list-based approaches to content filtering and blocking – that is, false positives. As the cybercriminal is able to jump from one IP address to the next faster than the lists are updated and deployed, the next owners/users of the IP addresses are the ones who are actually subjected to the blocking, instead of the cybercriminal. If the cybercriminals were so inclined, they could subvert the IP blacklisting technology and turn it into an efficient denial-of-service (DoS) tactic for extortion purposes.

6. The common ISP infrastructure is not designed to process a large number of DNS exceptions or block a substantial number of IP addresses, leading to concerns of whether the proposed solutions would scale. Building a large number of exceptions into the DNS infrastructure could potentially impact the Internet’s overall performance and reliability while creating operational concerns for many ISPs. Of course, email servers typically use IP blacklists as a first line of defense against spam and these lists usually contain millions of IP addresses. However, unlike the traffic passing on networks, spam filtering is not conducted in real time.

   The problem is exacerbated because there are so-called “fast flux” techniques that cybercriminals use to rapidly cycle through many thousands of IP addresses at a time, some of which are tied to unwitting end users infected with malware. Filtering traffic of a great many IP addresses on a real-time basis will place a substantial burden on the existing infrastructure and will not work in practice. Moreover this will be further exacerbated by the current deployment of the next generation of IP addressing, IP version 6 (IPv6), which requires many more IP addresses and longer IP address strings be built into the blacklist. The same considerable impact would be created by performing DNS filtering on a more granular basis, such as at the sub-domain or sub-directory level, which may require a more substantial number of exceptions to be built into the DNS infrastructure.

7. Blocking access to specific sub-directories such as http://www.example.com/bad/, while allowing the similar http://www.example.com/good/, will require a fundamental shift in the architecture of the Internet in the United States. It will require a veritable sea change from current standard operating procedure. This architectural shift would be enormously expensive and error prone while slowing achievable broadband access speeds. Such content inspection also would likely be met with a high degree of user anxiety, especially given the powerful level of user tracking it would enable.

   Successfully implementing URL blocking is more difficult than DNS blocking due to the complexity and fluidity of the underlying HTTP protocol, and the huge (and growing) number of evasion vectors. Maintaining extensive up-to-date lists of URLs to be blocked and filtered is many times more difficult than maintaining IP blacklists and domain name blacklists – both of which have consistently failed to stop professional cybercriminals. It would be trivial to apply evasion techniques, such as fast-flux, double-flux and domain-flux, and implement agile "URL fluxing" technologies.

   The forced adoption of such techniques would pose no significant pain to cybercriminals or others seeking to circumvent these controls but would cause considerable trouble for those charged with blocking and filtering illicit content as significant, new complexity would be added to the problem space. Accomplishing this in real time would require hardware-level implementations of efficient search algorithms that would economically parse such lists and block URLs, a need well beyond presently deployed commercial capabilities.

As tools to fight copyright infringement, DNS filters, IP address filters, and sub-directory filters will likely expose the Internet and its users to greater security risks and a broad range of other negative effects. Blocking by name or IP address in networks is not effective and does not scale well. It has not worked even in countries where the government directly controls the Internet.

We would like to note that MAAWG Senior Technical Advisor David Dagon is one of the authors of an excellent white paper that further explores these concerns, "Security and Other Technical Concerns Raised by the DNS Filtering Requirements in the PROTECT IP Bill," published in May 2011 (http://domainincite.com/docs/PROTECT-IP-Technical-Whitepaper-Final.pdf). We have also included below several other links to reference materials to assist you in your work.

If you have any questions or concerns and require additional information, please feel free to contact me.

Sincerely,
/signed/
Jerry Upton, Executive Director
Messaging Anti-Abuse Working Group (MAAWG)
jerry.upton@maawg.org
http://www.maawg.org

[1] Manos Antonakakis, Roberto Perdisci, David Dagon, Wenke Lee and Nick Feamster. "Building a Dynamic Reputation System for DNS," at the 19th USENIX Security Symposium, Washington D.C., August 11, 2010. http://www.usenix.org/event/sec10/tech/full_papers/Antonakakis.pdf

[2] DNSChanger Malware http://www.fbi.gov/news/stories/2011/november/malware_110911/DNS-changer-malware.pdf

[3] David Dagon, Niels Provos, Christopher P. Lee, Wenke Lee. "Corrupted DNS Resolution Paths: The Rise of a Malicious Resolution Authority," NDSS 2008. http://www.citi.umich.edu/u/provos/papers/ndss08_dns.pdf

[4] Manos Antonakakis, David Dagon, Luo Xiapu, Roberto Perdisci, Wenke Lee and Justin Bellmor. "A Centralized Monitoring Infrastructure for Improving DNS Security," 13th International Symposium on Recent Advances in Intrusion Detection (RAID 2010), Ottawa, Ontario, Canada, September 15-17, 2010. http://www.springerlink.com/content/856n3877xg261875/