BROOKINGS QUALITY. INDEPENDENCE. IMPACT.

Paper | November 15, 2011

Cybersecurity in the Balance: Weighing the Risks of the PROTECT IP Act and the Stop Online Piracy Act

By: Allan A. Friedman

Executive Summary

Cybersecurity has dominated headlines and the attention of American policymakers. The challenge is not in recognizing the problem, but in understanding how to balance cybersecurity efforts with other policy priorities and scarce resources. Two new bills designed to combat foreign websites that infringe on American intellectual property present one of the first such decisions to Congress: how can we balance the defense of cyberspace and defense against online piracy when the two conflict?

The Senate bill S.968, or the PROTECT IP Act, and the House bill H.R. 3261, the Stop Online Piracy Act, have raised a great deal of controversy. This paper does not deal with the questions of economic value, free expression or other issues raised by advocates on both sides. Instead, I highlight the very real threats to cybersecurity in a small section of both bills in their attempts to execute policy through the Internet architecture. While these bills will not "break the Internet," they further burden cyberspace with three new risks. First, the added complexity makes the goals of stability and security more difficult. Second, the expected reaction of Internet users will lead to demonstrably less secure behavior, exposing many American Internet users, their computers and even their employers to known risks. Finally, and most importantly, these bills will set back other efforts to secure cyberspace, both domestically and internationally. As such, policymakers are encouraged to analyze the net benefits of these bills in light of the increased cybersecurity risks.

Risks of Tampering with the Network

The Domain Name System (DNS) is a critical part of the Internet infrastructure, not just for the user seeking to access web pages, but for almost any operation, research question or network maintenance tool used to cross between organizational and network boundaries. Some interference with the DNS is not unheard of, but it should be done only after careful consideration, and with the full participation of Internet stakeholders.

The bills call for operators of DNS resolvers to "prevent the domain name described in the order from resolving." This is, in effect, lying. As we shall see below, this may sometimes be acceptable, but again must be done with care so as not to interfere with other aspects of network operation.

The broader Internet community has had the chance to judge the appropriateness of other attempts to return misleading results. Some network operators take advantage of imperfectly typed URLs to direct users to a landing page, rather than return the expected error message Non-Existent Domain (NXDOMAIN). A browser receiving the result NXDOMAIN might return an error “server not found.” With a DNS redirect, however, the user is taken to a search page that may assist her, but may also display advertisements. One vendor who enables this capacity claims that a service provider can earn $1-3 per subscriber with this service.[i] While DNS redirect for this purpose is not uncommon, many Internet experts do not view it favorably. Internet Corporation for Assigned Names and Numbers’ (ICANN) Security and Stability Advisory Committee (SSAC) cautioned that interfering in DNS responses “can create unpredictable responses,”[ii] and another ICANN advisory group concluded that the practice “create[s] a reasonable risk of a meaningful adverse effect on security and stability.”[iii] The SSAC has recommended that new top level domains be prohibited from using redirection.[iv] Clearly, this practice is viewed with apprehension by the body governing the domain name system.

Part of the threat of redirects is the potential for malicious misuse. The DNS system is based on trust between resolution servers. If an intermediary between the client and the authoritative server is untrustworthy, they can inject an incorrect record, diverting the client to a server other than the intended Internet resource. To make this system more trustworthy, the Internet Engineering Task Force (IETF) developed the Domain Name System Security Extensions (DNSSEC), which uses a set of chained cryptographic signatures to establish trust between the authoritative name server (such as the .com servers) and the recursive resolving servers used to translate from a desired URL to the IP address. This protocol allows correct responses to be provably valid, and incorrect responses to be identified as false. DNSSEC is seen as a needed security improvement for the Internet by both technical experts and the U.S. government. U.S. officials have viewed DNSSEC as important for its own systems, as well as the commercial Internet, since at least 2003. Deployment is proceeding slowly, but with the coordination and support of public and private efforts.

Because DNSSEC is designed to prevent malicious redirection of DNS traffic by verifying that DNS responses have not been tampered with, other forms of redirection will break the assurances from this security tool. Engineers from Comcast, in a circulated IETF working paper, clearly state, “It is critically important that service providers understand that adoption of DNSSEC is technically incompatible with DNS redirect.”[v] If the client is configured to recognize DNSSEC responses, any intercept will trigger the responses of an attempted man-in-the-middle attack. For the purposes of the bills in this paper, this response may be thought to have little policy impact since the goal is to prevent access in the first place. There are two adverse consequences, however. The first is that, without a reliable and standardized warning mechanism, the user may be unable to distinguish between malicious and illegal resources. The second is that one acceptable response to a DNSSEC failure is to query other recursive resolvers to confirm that the resource is not valid and available. This could violate the goals of the bills since these servers may be outside the jurisdiction of the United States.

It is important to acknowledge that DNS redirection may not always be bad for cybersecurity. Indeed, some domains are known to be security risks, hosting malware or serving as a critical link in the communication and coordination of botnets. As researchers identify which domains pose risks, DNS administrators may want to block them. A new tool called Response Policy Zones (RPZ) allows administrators to select lists of domains with bad reputations (assembled by anyone they might trust) and block their users.[vi] RPZ, designed to counter malicious behavior online, essentially creates the functionality called for in the bills to block domains specified by a trusted third party, with the potential to redirect the browser to an arbitrary notice page. However, there are key differences between RPZ and the bills' proposals.

First, RPZ engineers acknowledge that, as it exists, there is no easy way to make RPZ work well with DNSSEC. This will ultimately require some modification to DNSSEC to incorporate the error messages following an intercepted query. But because DNSSEC will take some time to fully deploy at the user level, there will be time to explore the most efficient means to implement this change. And because these protocols are implemented in voluntarily by network administrators trying to maximize the security of their networks, an appropriate balance can be found by each administrator.

Second, the legal mandate for the bills' block-list increases the complexity of the DNS network administration. PROTECT IP applies to every "operator of a non-authoritative domain name system server," including local ISPs and even small businesses that run their own networks. Each network must have the capacity to easily alter what can be accessed on their network, regardless of the preferences of the network administrator and her resources and capacities. Security expert Susan Landau observes that adding points of insertion or observation can dramatically alter the security of a system.[vii] Perhaps the largest difference, of course, is that RPZ is voluntary—and ideally in the interest of the user. In a competitive market, users who find one service provider's implementation too broad or narrow can go to another. If the users do not believe that a black list is in their interest, they will find ways around it, as explored below.

Tinkering with DNS by mandating false responses may not break the Internet, but it certainly bends it, and introduces new complexities. The security community understands that these risks must be carefully studied before there is widespread deviation from the accepted standards.

Unintended Consequences Introduce New Risks

By preventing American users from accessing foreign websites, the bills' clear aim, insofar as they deter Americans from supporting behavior that infringes on intellectual property, is to stop piracy. Past efforts to halt piracy do sometimes have limited success, but they also succeed in changing the behavior of millions of Americans to find other means of accessing this content. Any analysis of these bills must therefore explore the consequences of these new behaviors. The DNS blocking of foreign websites is not only trivial to defeat, but many work-arounds will definitely have dangerous unintended consequences.

The bills seek to block access to foreign infringing websites by preventing American domain name servers from translating the infringing domain name into its Internet address. This is trivial to defeat on many levels, as has already been chronicled widely.[viii] One of the easiest and most direct methods is simply to use a DNS server that is located outside of the bills' jurisdiction in another country. This requires minimal computer expertise.[ix]

Before exploring the harms of using a non-trusted DNS server, is there any reason to expect users to change their behavior en masse? The data says yes. Those seeking infringing content have always responded to legal and technical countermeasures by shifting their habits. From Napster to Kazaa to LimeWire to BitTorrent to illegal streaming websites, users adapt by the millions. When the RIAA succeeded in shutting down the peer-to-peer client LimeWire in 2010, use of a similar client FrostWire more than doubled within 3 months.[x] When Sweden passed a law requiring service providers to turn over identity information on infringers, demand for both paid and unpaid anonymity services skyrocketed "beyond all expectations."[xi] It would be incredibly naïve to expect anything other than attempts to evade DNS blocking, and using DNS servers outside the U.S. is the easiest path.

This introduces huge risks to American Internet users. These DNS servers can sit as the "man-in-the-middle" on all Internet transactions, allowing the possible compromise of almost any Internet transaction. The attacker can pass along the legitimate website during the attack, preventing the user from realizing that an attack is ongoing. Even the use of encryption (such as SSL or https) will not help. The attacker can not only compromise web traffic, but email as well. There already exists malware that forces victims to use remote, rogue DNS servers to maliciously redirect traffic to key financial websites.[xii] The operators behind these attacks will undoubtedly seek to gain further traffic to these servers.

The risks of malware, financial fraud and espionage will not fall exclusively on the users guilty of infringement. Rather, they will be shared by anyone who shares a network with these users. It is easy to imagine a teenager altering the family PC to access a foreign infringing domain, but leaving the computer compromised for the family's other uses, including banking, accessing government websites and even work.

Even if the foreign DNS servers are benign and supervised by an open source community, there is still a destabilizing effect. Content Deliver Networks (CDNs), such as Akamai, that make it easier and cheaper to send large files over the Internet by replicating it many times across the Internet. Some CDNs use the DNS request to determine the closest and most efficient content server.[xiii] Foreign domain requests will confuse this system, leading to greater inefficiencies and instability. Interestingly enough, this can lead to slower content deliver from paying, legitimate sites, further increasing the incentives for infringement. ISPs also use local DNS information to better manage their networks; the less complete this data is, the less informed decisions will be.

Cybersecurity Policy

Many cybersecurity issues require international coordination. The GAO has identified 19 international organizations relevant to Internet governance, each with a different set of stakeholders and counter-parties.[xiv] In each forum, the United States must be seen as a good faith actor, seeking to promote global security in cyberspace without advancing alternate agendas. The policies must not be perceived as conflicting with other values, such as openness and limited governance. While many would agree that any measure is acceptable to prevent intellectual property infringement, some might see this as a signal of what values the U.S. will emphasize—and what it will implicitly devalue. As the Council on Foreign Relations' Rob Knake notes, "If the United States fails to provide the leadership necessary to address the security problems, other states will step in."

It is important to remember that the United States occupies a unique position in Internet governance. The Internet was invented here, and many of its key institutions remain affiliated with the federal government. U.S. companies support much of the Internet architecture. This dominant position has not gone unnoticed from those who would prefer a more globally representative governing structure. This would necessarily involve reducing U.S. influence in key security-relevant bodies.

American representatives across the government have worked hard to focus the international dialogue on "cybersecurity," without permitting discussion to be reframed as "information security," which can include policing of content instead of just actions. This position is undermined by domestic bills that focus on content at the expense of cybersecurity. It will be hard to argue with other nations that discussions should focus on preventing malicious behavior, rather than stamping out illegal content—a category into which many other nations put political speech. Indeed, other observers have pointed out the challenges in reconciling these anti-infringement bills with America's stated agenda of Internet Freedom, particularly SOPA's anti-circumvention prescriptions.

Lastly on the international front, it is important to remember the difficulties in perfectly mapping the Internet to national boundaries. It is highly likely that DNS blocking will spill over into other countries. In 2010, China's internal attempts to block certain websites via DNS spilled over to the broader Internet.[xv] The U.S.-China Economic and Security Review Commission's Annual Report to Congress noted, "The implications of China's effort to impose 'localized' restrictions to something as inherently global in scope as the Internet."[xvi] Since the United States' networks are so centrally positioned in the global information infrastructure, there is a good chance that foreign DNS queries will pass through U.S. resolvers. Other countries may object to our unilateral enforcement without adequate international normalization or even discussion.

Domestically, the bills pose three principle risks, based on expectations and trust. First, by mandating an unpopular enforcement mechanism to the ISP, users may grow to trust their ISPs less, even as service providers play an increasingly large role in American cybersecurity policy. If the user is treated as an enemy, it makes winning consumer acceptance for other efforts all the more difficult. A recent proposal from the National Institute of Standards and Technology would have ISPs detect botnets on customers' machines and work with them for remediation. This requires user trust and a belief that user security is a higher priority for the service provider than other business interests. The ISPs also depend on user trust to make the entire network better off. By studying pooled DNS lookups across a large set of users, security researchers can learn a great deal about attacks based on data referred to as Passive DNS. This data will be incomplete if users evade the DNS blocks en masse, as discussed above.

Expectations also drive investment, and new investment can happen under the jurisdiction of these bills, or outside the country. Without engaging in the larger debate of how this bill will impact long-term economic growth, there is a security issue in jurisdiction. If the provisions in the bills that allow rights holders to go after domestic assets drive these assets offshore, they can make the fight against other illegal digital activities harder to pursue. As new Top Level Domains are issued by ICANN, their supporters may push for offshore control. Similarly, if attacks against website monetization tools, including ad networks and payment networks become too aggressive, offshore alternatives will emerge. American law enforcement and intelligence will have less leverage over these. If one acknowledges that there are cybercrime issues other than intellectual property infringement, such as child pornography or financial fraud, then a long-term enforcement tradeoff will be made. Making it more efficient to drive potential wrongdoing away from America's jurisdiction may ultimately hinder law enforcement.

Finally, and perhaps most importantly, the bills set a certain expectation with respect to the relative importance of cybersecurity versus industry profitability. There is always a tradeoff between economic efficiency and security. As technology evolves, each sector of the economy discovers new risks, just as they discover new benefits. These bills offer an explicit tradeoff: protecting the economic value of intellectual property from a narrow type of infringement against a larger and more diffuse set of security priorities.

Cybersecurity policymakers will only encounter this tradeoff more frequently. The costs of the status quo must be measured against the security risks of mandating a change in the Internet architecture. Unfortunately, it is always easier to estimate actual business models than uncertain security risks. This is why market solutions for cybersecurity are particularly challenging.[xvii] If securing the power grid harms the business model of energy companies, will Congress still act to ensure our critical infrastructure is less vulnerable to attack?

Will Cybersecurity Be a Priority?

Threats from cyberspace present serious challenges, yet no one suggests that we turn off the Internet to protect ourselves. Similarly, while digital entertainment is a key part of the economy, few argue that we lock down all networks and devices for perfect enforcement of intellectual property. The question is where the balance will be struck.

The risks from the proposed policies are diffuse, and the harms of a perturbed ecosystem, exposed Americans and a more difficult cybersecurity agenda lie in the future. Yet they are real—and will have concrete, negative impacts on our nation's ability to defend itself, endangering everyone from the average user to shapers of international policy. This will be the first legislation that pits our cybersecurity priorities against entrenched economic interests, highlighting a very real social choice. Congress' actions on PROTECT IP and SOPA will offer some insight into whether policymakers are genuinely prepared to take cybersecurity seriously.

[i] Xerocole Solutions. http://www.xerocole.com/solutions/

[ii] "SAC 032 Preliminary Report on DNS Response Modification," ICANN Security and Stability Advisory Committee, June 2008; www.icann.org/en/committees/security/sac032.pdf.

[iii] ICANN Registry Services Technical Evaluation Panel Report on Internet Security and Stability Implications of the Tralliance Corporation search.travel Wildcard Proposal (2006)

[iv] "SAC041: Recommendation to Prohibit Use of Redirection and Synthesized Responses by New TLDs," ICANN Security and Stability Advisory Committee (2009) www.icann.org/en/committees/security/sac041.pdf.

[v] Creighton, T., Griffiths, C., Livingwood, J., and Weber, R. "DNS Redirect Use by Service Providers. Internet Draft draft-livingood-dns-redirect-03." (2010) http://tools.ietf.org/html/draft-livingood-dns-redirect-03

[vi] ISC. BIND 9 Administrators Reference Manual, 2011. See 6.2.16.19 and 6.2.16.20

[vii] Landau, Susan. Surveillance or Security? The Risks Posed by New Wiretapping Technologies. MIT Press, 2011

[viii] See, e.g., Wilson, Drew. "8 Technical Methods That Make the PROTECT IP Act Useless." www.zeropaid.com/news/95013/8-technical-methods-that-make-the-protect-ip-act-useless/

[ix] See, e.g., http://windows.microsoft.com/en-US/windows7/Change-TCP-IP-settings.

[x] Sandoval, Greg. "Study: LimeWire demise slows music piracy" http://www.news.cnet.com/8301-31001_3-20046136-261.html

[xi] Simpson, Peter Vinthagen. New law increases demand for anonymous web surfing www.thelocal.se/18658/20090403/#

[xii] David Dagon, Chris Lee, Wenke Lee, Niels Provos . “Corrupted DNS Resolution Paths: The Rise of a Malicious Resolution Authority”, , Proc. 15th Network and Distributed System Security Symposium (NDSS), 2008.

[xiii] Vixie, Paul. What DNS is Not. ACM Queue, 2009. http://queue.acm.org/detail.cfm?id=1647302.

[xiv] Cyberspace: United States Faces Challenges in Addressing Global Cybersecurity and Governance. GAO-10-606 July 2, 2010

[xv] Zmijewski, Earl. "DNS: When Governments Lie." http://www.renesys.com/blog/2010/11/dns-when-governments-lie-1.shtml

[xvi] USCC. 2010 Annual Report to Congress. http://www.uscc.gov/annual_report/2010/Chapter5_Section_2(page236).pdf

[xvii] Friedman, Allan. Economic and Policy Frameworks for Cybersecurity Risks. (2011) www.brookings.edu/papers/2011/0721_cybersecurity_friedman.aspx

Author

Allan A. Friedman
Fellow, Governance Studies
Research Director, Center for Technology Innovation