DNS Filtering and S.3804, "Countering Online Infringement and Counterfeiting Act"
Dan Kaminsky, Computer Security Researcher[1]
Finder and Fixer of the Kaminsky Bug[2]

My core concern is one of unintended consequences.

Put simply, if running antivirus software prevented users from listening to pirated copies of the latest Lady Gaga album, users would not run antivirus software. There has long been a bright line in computer security technology -- do not subvert the will of the user, for the user is in the position to opt out of all protections.

By sanctioning the use of DNS filtering to combat copyright and trademark infringement, this bill will directly cause users to opt out of using their ISP's name servers.[3] This will lead to more hacks against American assets, for a number of reasons.

First, as the Center for Democracy and Technology correctly notes, changing name servers is a trivial task, taking less than one minute. Which server a user chooses for DNS resolution, however, has consequences. One could easily imagine users being told that to access "The Pirate Bay", they should change their name server to one outside their ISP, and outside the United States. These foreign servers would then not only be used for locating pirated resources, but legitimate ones as well -- bank sites, e-commerce sites, even search engines.

Alternatively, users might abandon shared name servers entirely, opting to running their own locally (think of this as a "Pirate Bay Helper" application, itself which might be infected). The DNS depends on shared servers to manage load. Incentivizing large numbers of users to abandon the shared arrangement could have major implications for network stability.

Two years ago, I was part of a major effort to ensure people could trust their own name servers when looking up their banks, their e-commerce sites, or their search engines.[4] This bill would completely undermine that effort and instead create greater security and stability risks for Internet users and the DNS.

Note that it is extraordinarily easy for users to avoid DNS filters. In countries outside the United States where large-scale filtering regimes are in place, we see

---

[1] http://en.wikipedia.org/wiki/Dan_Kaminsky
[2] MIT Technology Review, "The Flaw at the Heart of the Internet," November/December 2008, by Erica Naone, available at http://www.technologyreview.com/web/21537/. *See also,* http://www.wired.com/techbiz/people/magazine/16-12/ff_kaminsky
[3] Section (e)(2)(b)(i) of the bill would impose DNS filtering obligations. That provision authorizes the issuance of a court order requiring service providers and DNS server operators to "take technically feasible and reasonable steps designed to prevent a domain name from resolving to that domain name's Internet Protocol address".
[4] *Id.*

tremendous awareness and adoption of proxying and VPN technologies, even among the nontechnical. The proposed filter will have no impact on the piracy rate -- and it still wouldn't, even if it were ten times more aggressive. Even users that have no interest in infringing content but object to DNS filtering by their local ISP would gravitate toward alternative DNS servers.

DNS filtering is used now in very limited circumstances. It is one of the few tools that defenders possess to manage botnets and other very large-scale cyberattacks against the Internet population. The best place to deploy DNS filters is at the users' ISP name server. But these filters will become useless once users abandon their ISP name servers.

We will also lose a significant amount of our "eyes and ears" with respect to attacks. DNS servers are tremendously useful vantage points from which to monitor the overall activity of the network. They provide an extraordinarily valuable, even predictive, data stream regarding malicious behavior. Losing this stream would materially degrade our ability to secure cyber space.

Had this law been in place when we worked to patch major ISP name servers several years ago, it would have severely hampered our success in actually getting safe code to users, since they would have been using other servers, with unknown configurations. Now, with DNSSEC finally offering the real fix for cache poisoning, we see a proposal that will cause users to avoid the very servers we've spent a decade trying to secure and to get people to use.

There is a final concern -- and it's not the constitutional worry. DNS is a global namespace, managed globally, operated globally. Unilateral action by the United States threatens similar action by other state actors, in forms that are difficult to predict but very clearly not of the form that can be managed through the present global forums run by ICANN.

Ultimately, there are many layers at which piracy can be attacked. Operating at this layer has harmful unintended consequences that will make Americans less safe. DNS filtering is a blunt instrument, a hammer in place of a scalpel.

The DNS works remarkably well right now. It is a core element of how commerce functions. We should not be interfering with this working system, especially not without deliberation and research into unintended consequences.