KEEPING THE INTERNET
OPEN • INNOVATIVE • FREE

www.cdt.org

CENTER FOR DEMOCRACY
& TECHNOLOGY

1634 I Street, NW
Suite 1100
Washington, DC 20006

P +1-202-637-9800
F +1-202-637-0968
E info@cdt.org

THE PERILS OF USING THE DOMAIN NAME SYSTEM TO ADDRESS UNLAWFUL INTERNET CONTENT

September 2011

Governments and law enforcement agencies are increasingly grappling with how best to address unlawful content and activity online. In the United States, there has recently been considerable focus on using the domain name system (DNS) to go after websites associated with unlawful content. Since late June 2010, law enforcement agencies have executed seizure warrants for over 100 domains associated with copyright and trademark infringement as part of "Operation In Our Sites."[1] The "PROTECT IP Act," introduced in the U.S. Senate, would give law enforcement the ability to bring actions against foreign domain names and to compel Internet service providers (ISPs) and other DNS service providers to block domain-name lookup requests.[2]

CDT believes that the these approaches to unlawful online activity – while perhaps attractive to those seeking to block particular content – would be largely ineffective yet carry significant risk of collateral damage. Taking down and blocking domain names risk suppressing lawful expression; exacerbating cybersecurity risks; and encouraging cross-jurisdictional disputes in which each country tries to use the domain name system to assert domestic jurisdiction over foreign websites. This paper briefly discusses the ineffectiveness and risks of domain-focused enforcement.

A. Ineffectiveness

Domain-name seizure and blocking can be easily circumvented, and thus will have little ultimate effect against unlawful content that users want to access.

The DNS performs a relatively simple function: translating text URLs (like www.cdt.org) into machine-readable IP addresses (like 174.143.118.160). Seizing a domain name involves ordering the relevant registrar or registry to effectively revoke the website's domain name registration, thus preventing the site from continuing to use that particular name. Blocking a domain name involves ordering a domain name lookup service (for most users, a function performed by their ISP) not to respond to any user request to look up the IP address associated with that name.

---

[1] ICE, "'Operation In Our Sites' targets Internet movie pirates: ICE, Manhattan U.S. Attorney seize multiple Web sites for criminal copyright violations," Press Release, June 30, 2010, http://www.ice.gov/news/releases/1006/100630losangeles.htm.

[2] Preventing Real Online Threats to Economic Creativity and Theft of Intellectual Property Act, S. 968, 112th Congress (2011).

Significantly, neither seizing nor blocking a website's domain name *removes* the site – or any infringing content – from the Internet. The site and all its contents remain connected at the same IP address. And there are numerous ways a targeted site may still be reached.

In the case of a domain-name seizure, the site's operator could simply register a new domain name for the site. For example, most of the sports-streaming sites connected to ten domains seized in the U.S. in February quickly reappeared and are easily located at new domains. Alternatively or in addition, the site's operators could publicize its IP address, which users could then bookmark in lieu of saving or remembering the domain name.[3] Or a site's operators could distribute a small browser plug-in or other piece of software to allow users to retrieve the IP addresses of the operators' servers. Such simple tools would make the process of following a site around the web virtually automatic.

The same tactics could be used to evade domain-name blocking. In addition, a site's users could easily switch DNS-lookup providers to avoid blocking orders. Savvy users could set up local DNS resolvers on their own computers, thus avoiding any DNS servers that have been ordered to block. Alternatively, third-party public DNS servers are widely available, and more would inevitably spring up outside the blocking country to avoid being subject to blocking orders. For Internet users, pointing DNS requests to these unfiltered servers would be simply a matter of updating a single parameter in their operating systems' Internet settings. For users to whom this seems complicated, software tools could easily automate the process.

All of these circumvention techniques are likely to occur if domain-name seizure and blocking become widespread. To the extent that sites hosting unlawful content have a highly motivated and relatively savvy user base (as is often the case for sites and networks hosting copyright-infringing material), word would spread quickly as to how best to circumvent any blocking. This means that any impact from seizing or blocking domain names is likely to be ephemeral at best.

B. Overbreadth: impact on lawful expression

The seizure and blocking of domain names would almost certainly affect lawful speech, for several reasons.

When domain-name tactics are used against websites with a mix of lawful and unlawful content, *all* the content is affected; there is no way to narrowly target the unlawful content only. This stands in sharp contrast to notice-and-takedown provisions currently in place in many countries. These processes are typically used in the copyright context to address specific infringing material – and *only* that material. Enforcement actions targeting a domain name itself would not be so narrowly targeted; they would affect anything and everything associated with that domain.

Moreover, a domain name frequently encompasses much more than just an individual website. Many web hosting services are constructed in a way such that thousands of individual sites, maintained by thousands of individuals, are hosted at subdomains sharing a single parent domain name. For example, the service might be located at "webhost.com" and the individual sites might be "joe.webhost.com" and "bob.webhost.com." In addition, websites often share

[3] This is exactly what happened when the provider of Wikileaks's DNS service provider terminated the controversial site's account in December 2010; the IP address was immediately and widely available. *See* Rob Pegoraro, "WikiLeaks sinks, resurfaces (repeat as necessary)," *Washington Post* Faster Forward blog, December 3, 2010, http://voices.washingtonpost.com/fasterforward/2010/12/wikileaks_sinks_resurfaces_rep.html.

their domain names with non-web hosts, such as email and instant messaging servers. All of this speech stands to be affected if the domain name is seized or blocked.

Indeed, a concrete example occurred in February 2011, when a U.S. law enforcement agency mistakenly seized the domain "mooo.com," for hosting child sexual abuse images. Mooo.com turned out to be the parent domain of thousands of innocent and unrelated subdomains.[4] The owner of mooo.com allows individuals to register subdomains, which they can then point to any IP address. That means the mooo.com domain name is effectively subdivided and shared among numerous, entirely independent users. The content hosted at any particular subdomain is wholly separate – hosted on different servers with different IP addresses – than the content hosted at other subdomains or at the first-level "mooo.com" domain itself. But because of illegal content allegedly present at one such subdomain, *all* were seized and redirected to a U.S. government banner announcing that the domain had been seized for violating child pornography laws.

The risk of sweeping in lawful content is made worse if seizure or blocking orders are issued without a full adversarial hearing. Large-scale use of a one-sided process, under which domain name owners get no opportunity to defend themselves before their names are blocked or seized, creates significant potential for mistakes or overaggressive action. Again, several examples from the recent seizures in the U.S. highlight this risk: the seized sites include several music blogs who claim they had obtained the allegedly infringing material directly from rightsholders for promotional purposes,[5] as well as a Spanish site that has twice been found non-infringing by Spanish courts.[6]

In sum, seizing and blocking domain names would impede access to some lawful material that simply shares a domain name with infringing material. This overbreadth makes the tactics highly suspect from the perspective of online freedom of expression.

C. Technical impact and cybersecurity

Seizing and blocking domain names presents a number of technical challenges that could have an impact on the Internet's reliability, security, and performance.[7]

First, for ISPs, compliance with blocking orders may come at the expense of implementing the DNS Security Extensions (DNSSEC). For over 15 years, Internet engineers have been working to develop and implement a set of standards for addressing security flaws in the domain name system. But having DNS lookup providers either pretend a site does not exist or redirect users

---

[4] Thomas Claburn, "ICE Confirms Inadvertent Web Site Seizures," *Information Week*, February 18, 2011, http://www.informationweek.com/news/security/vulnerabilities/showArticle.jhtml?articleID=229218959&cid=RSSfeed_IWK_All.

[5] Ben Sisario, "Music Web Sites Dispute Legality of Their Closing," *New York Times*, December 19, 2010, http://www.nytimes.com/2010/12/20/business/media/20music.html.

[6] Nate Anderson, "US Customs begins pre-Super Bowl online mole-whack," *Ars Technica*, February 2, 2011, http://arstechnica.com/tech-policy/news/2011/02/us-customs-begins-pre-super-bowl-mole-whacking.ars; *see also* Mike Masnick, "Homeland Security Seizes Spanish Domain Name that Had Already Been Declared Legal," *Techdirt*, February 1, 2011, http://www.techdirt.com/articles/20110201/10252412910/homeland-security-seizes-spanish-domain-name-that-had-already-been-declared-legal.shtml.

[7] A group of prominent DNS engineers has issued a paper that discusses these concerns in greater detail. S*ee* Steve Crocker et. al, *Security and Other Technical Concerns Raised by the DNS Filtering Requirements in the PROTECT IP Bill*, May 2011, http://domainincite.com/docs/PROTECT-IP-Technical-Whitepaper-Final.pdf.

to a site they have not requested (such as to a site saying "access to the site you were seeking is being blocked due to illegal content") is flatly inconsistent with DNSSEC. The incompatibility is technical; DNSSEC uses cryptography to prevent DNS responses from being tampered with or falsified. A DNS resolver using DNSSEC simply is not able to give a cryptographically signed response that is false. DNS lookup providers could try to avoid the incompatibility by declining to respond to certain DNS requests at all, but this carries performance and user-experience drawbacks that providers might prefer to avoid.

Blocking at the DNS lookup-provider level carries security risks for Internet users beyond the tension with DNSSEC. Most users today rely on their ISP to perform domain-name lookup functions. But as explained above with regard to ineffectiveness, switching to another lookup provider is trivial. The more ISPs and other major DNS providers are required to block lookup requests for websites that users want to reach, the more users will switch to independent, non-ISP DNS servers. And critically, they may not switch to other trustworthy DNS providers, but to DNS services located outside of the reach of blocking orders – likely to DNS servers operated by the very purveyors of the illegal content they wish to reach.

This would do more than just render service-provider-level domain-name blocking ineffective. ISPs' DNS servers offer a crucial window into network usage; migration away from these servers would undermine ISPs' ability to observe and track botnet activity and other cybersecurity threats on their networks.[8]

In addition, it would put users at the mercy of potentially unscrupulous foreign DNS servers, which could redirect user traffic for phishing or botnet purposes. Though they may be unaware of it, users place an enormous amount of trust in their DNS provider to route requests to the proper sites. ISPs have incentive to maintain that trust, but other DNS operators – especially those with an interest in evading the blocking of sites dedicated to commercial infringement – will likely not share that same incentive. By creating strong incentives to rely on potentially untrustworthy DNS providers, the widespread use of domain-name seizure and blocking would create new and very dangerous opportunities for security risks and crime online.

Finally, encouraging many users to rely on out-of-country DNS servers could undermine the efforts of content distribution networks (CDNs, such as Akamai) to improve the overall speed and efficiency of the Internet as a whole. Some CDNs rely on the approximate location of users' DNS lookup servers (based on IP address) to choose the best location from which to deliver content. As users change their DNS settings to use foreign nameservers, this signal will become a less reliable proxy for a user's location. For example, a CDN might assume a Canadian user using a Russian DNS provider is in Russia, undermining the benefits of CDNs and distributed hosting and increasing Internet congestion.

These security and reliability harms flow directly from the use of domain-name remedies to address objectionable content. In light of how ineffective the approach is likely to be, this should raise serious questions as to whether the approach is worth the risk.

[8] *See* Statement of DNS security researcher Dan Kaminsky regarding S. 3804, available at http://www.publicknowledge.org/files/docs/COICA_Kaminsky_letter.pdf.

D. Implications for jurisdiction

From an international perspective, widespread use of DNS blocking risks creating dangerous jurisdictional disputes that would threaten the stability of the Internet. If the practice were to become commonplace, states would likely seek to exercise seizure or blocking orders in cases where jurisdiction over the operator of a particular site is unobtainable. Different states may try to seize or block the domain names of websites that are locally unlawful but lawful where the website is hosted.

To take a concrete example, in 2000, a French court ruled that a Yahoo auction site (located at the Yahoo.com domain) violated French law because it contained postings for Nazi memorabilia.[9] A U.S. court refused to enforce that judgment, because the site's activity was lawful in the United States. Taking the domain-name approach, however, in the future a country with a similar complaint could try to seize or block the site's domain name. In the case of domain seizure, this would mean making the targeted domain unavailable for the entire world.

Enshrining domain-name seizure and blocking in statute could also serve as precedent for a variety of actions that are best characterized as censorship. Already, some countries erect national Internet "firewalls," in an effort to suppress access to certain speech. Over forty countries (and growing) now filter the Internet to some degree, in ways that are inconsistent with human rights standards most recently articulated by the U.N. Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression.[10] In countries where rule of law is weak or entirely absent, the global acceptance of domain-name seizure and blocking would open the door to serious misuse.

More broadly, embracing domain-focused remedies as an enforcement tool risks balkanizing the Internet and undermining its benefits as a global platform for communication. In addition, the use of domain seizure would signal acceptance for the proposition that countries have the right to insist on removal of content from the global Internet as a tactic for enforcing domestic laws.

Conclusion

CDT does not suggest that governments should not take action against unlawful online activity. But any action taken must be subject to a realistic cost-benefit analysis. The codification and widespread use of domain-name blocking and seizure would carry costs and risks that would far exceed their minimal impact. Thus the tactics are not appropriate tools for addressing unlawful online content.

---

[9] *UEJF and Licra v. Yahoo! Inc. and Yahoo France*, Tribunal de Grand Instance de Paris, May 22, 2000, http://www.juriscom.net/txt/jurisfr/cti/yauctions20000522.htm.

[10] "Report of the Special Rapporteur on key trends and challenges to the right of all individuals to seek, receive and impart information and ideas of all kinds through the Internet," A/HRC/17/27, May 16, 2011, http://daccess-ods.un.org/TMP/4928395.15209198.html.