CDT Warns Against Widespread Use of Domain-Name Tactics To Enforce Copyright

March 21, 2011

Policy Posts are in-depth analyses on current tech policy issues from CDT experts. Sign up to receive the latest Policy Posts here:

1. CDT Warns Against Widespread Use of Domain-Name Tactics to Enforce Copyright

A major current topic in the online copyright debate is what to do about "rogue websites" – that is, websites that exist for the purpose of enabling illegal activity, especially copyright infringement and counterfeiting. One prominent idea lately is to have law enforcement authorities seize or block the domain names of such websites. Since late June 2010, Immigration and Customs Enforcement (ICE) and the Department of Justice have relied on civil forfeiture authority, which allows for seizure of property believed to have been used in commission of a crime, to execute seizure warrants for over 100 domain names. Last fall, the Senate Judiciary Committee developed a bill (S. 3804, the "Combating Online Infringement and Counterfeits Act" or "COICA") which would have codified and expanded this practice. Similar legislation is likely to return in the current Congress, as both the House and Senate held hearings on the "rogue website" problem in recent weeks.

CDT supports the goal of reducing online infringement. Large-scale copyright infringement undermines First Amendment values in promoting expression and threatens the growth of new media and e-commerce. Websites whose main purpose and activity is to enable and promote infringement are true "bad actors" and deserve to be the target of law enforcement.

Nonetheless, CDT believes that legislation that would codify and encourage large-scale reliance on domain names as an enforcement mechanism would be a serious mistake. Meaningful law enforcement in this area requires, above all, catching and punishing actual criminals who operate "rogue sites." By contrast, focusing on domain names would prove ineffective at achieving any lasting reduction in infringement. At the same time, the domain-name approach would risk significant collateral damage.

CDT explained its concerns in a written statement it submitted for the record of the Senate Judiciary Committee hearing held in February, and again last week in testimony before the House Judiciary Subcommittee on Intellectual Property, Competition, and the Internet.

CDT Policy Post on Copyright Enforcement Trend [1]

CDT Comments to Department of Commerce's Internet Task Force Copyright Inquiry [2]

CDT Statement for Senate Hearing [3]

CDT Testimony for House Hearing [4]

2. Domain-name seizure and blocking will be ineffective at reducing infringement

Domain-name seizure and blocking can be easily circumvented, and thus will have little ultimate effect on online infringement.

The DNS performs a relatively simple function: translating text URLs (like www.cdt.org [5]) into machine-readable IP addresses (like 72.32.6.120). 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.

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 ICE seized 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. 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 United States 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. Infringement sites have a highly motivated and relatively savvy user base, and word will spread quickly as to how best to circumvent any blocking. The workarounds themselves are trivial and would quickly go viral, ultimately rendering the domain-name approach almost entirely ineffective.

3. Collateral Impact

The seizure and blocking of domain names would carry a number of collateral risks and costs.

Overbreadth / Impact on Lawful Speech: First, widespread use of such tactics would almost certainly affect lawful speech. For example, 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. Last year's COICA legislation, despite its purported focus on websites "dedicated to infringing activities," defined that phrase broadly enough to apply to multipurpose sites featuring a wide variety of content. Indeed, under the bill as drafted, user-generated content websites could be subject to domain-name seizure or blocking if even a small minority of users posted infringing material.

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. Non-web hosts, such as email and instant messaging servers, often share the domain as well. All of this speech stands to be affected if the domain name is seized or blocked. Indeed, a concrete example occurred in February, when ICE mistakenly seized the domain "mooo.com," which turned out to be a parent domain to thousands of innocent and unrelated subdomains. As a result, many small, legitimate websites had their traffic redirected to an ICE banner announcing that the domain had been seized for violating child pornography laws.

The risk of sweeping in non-infringing content is exacerbated when seizure or blocking orders are issued without a full adversarial hearing, as is the case under both the current ICE seizure process and the proposed COICA legislation. 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 ICE seizures 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, as well as a Spanish site that has twice been found non-infringing by Spanish courts.

The potential for overbreadth raises serious constitutional questions regarding the degree to which domain-name seizure and blocking can be narrowly tailored to affect infringing content. Moreover, domain-name seizure and blocking targets an instrumentality of speech (domain names) and creates a prior restraint, effectively trying to censor all future activity at a domain based on illegal activity in the past. Especially given how ineffective domain-name focused enforcement measures are likely be in achieving their stated goal, as discussed above, the approach could be vulnerable to a First Amendment challenge.

Technical Impact / Cybersecurity: Widespread seizing and blocking of domain names would present a number of technical challenges that could have an impact on the Internet's reliability, security, and performance.

For ISPs, redirecting users to a page reading "this website blocked due to infringement" could conflict with implementations of the DNS Security Extensions (DNSSEC), a security improvement just now rolling out after over 10 years of development. A DNS resolver using DNSSEC simply is not able to give a cryptographically signed response that is false.

Users' efforts to circumvent blocking orders may have technical and cybersecurity consequences as well. 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. But 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. 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. It could also undermine the effectiveness of content delivery networks (CDNs), which often rely on the approximate location of users' DNS lookup servers (based on IP address) to choose the best location from which to deliver content.

International Impact / Precedent: Enshrining domain-name seizure and blocking in a new statute would invite similar action from other countries, harming U.S. interests and undercutting diplomatic efforts to promote global Internet freedom.

Following the U.S. example, other countries could try to seize or block the domain names of U.S. websites that are lawful here but that are asserted to violate some foreign law. In the case of domain-name seizure, such action could render the targeted domain inaccessible for the entire world.

Moreover, this risk is not limited to repressive regimes. The scope of protection provided by the First Amendment remains the most expansive in the world, and speech protected in the United States remains proscribable in many other democratic countries. Local access to such speech remains a frustration to governments in those countries, and they would welcome a U.S.-based precedent to justify blocking it.

Setting such a precedent would also undermine US diplomacy. Over forty countries (and growing) now filter the Internet to some degree, and even liberal democracies are considering mandatory filtering and blocking regimes. Historically, the United States has been the strongest global voice against such balkanization of the Internet; the concept of a single, global Internet is a cornerstone of U.S. foreign policy on Internet matters. If the United States were to set the precedent that any country can order the blocking of a domain name if some of the content at that domain violates the country's laws, it is hard to see what credibility the U.S. would have as it urges other countries not to block access wherever they see fit.

This does not mean that the United States should not take action against online infringers and encourage other countries to do likewise. The concern is simply that trying to use domain names as

the means for fighting infringement would signal U.S. 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 – and nothing would limit the application of this approach to copyright infringement and counterfeiting.

NY Times on music blog seizure [6]

ArsTechnica on Spanish site seizure [7]

CDT blog post on Mooo.com seizure [8]

White House blog post on DNSSEC [9]

Security Researcher Dan Kaminsky on COICA's security risks [10]

4. Principles for a Sound Policy Approach

Fighting online infringement is a worthy goal. Based on the analysis above, however, CDT believes that large-scale reliance on enforcement tactics that target domain names would fail any cost-benefit test.

A sound policy approach in this area should focus first and foremost on catching and punishing true "bad actors." In the case of non-U.S. perpetrators, this will require cooperation with foreign governments. While such cooperation undoubtedly takes some effort, it ultimately offers the most effective approach, because it is the only way to ensure that the "bad guys" and the computer servers they use are actually taken offline for good.

To the extent policymakers believe new enforcement tools are necessary, they should look for remedies other than domain-name blocking and seizures. Cutting off infringers' sources of financial support would be one area to explore. New remedies should be subject to careful cost-benefit analysis, asking both how effective a measure is likely to be and what collateral impact it may cause. Remedies that aim to sidestep adversarial judicial process would, at a minimum, need to be narrowly tailored and contain carefully crafted procedural safeguards. As the experience with ICE seizures has already begun to demonstrate, any process with insufficient safeguards risks impairing lawful websites and speech.

Finally, it is important to keep in mind that a full strategy for reducing online infringement requires more than just the "stick" of law enforcement. One of the best defenses against infringement websites is the "carrot" of convenient, easy-to-use lawful choices for consumers to get the content they want in the form they want it. Policymakers should look for ways to encourage the legal marketplace. Public education is crucial as well. Modern information technology is here to stay and will continue to put powerful digital tools in the hands of the public. Inevitably, public norms and attitudes will play a major role in shaping how people choose to use the tools at their disposal. Consumers need better education about what copyright law prohibits and why infringement is both illegal and wrong.

Source URL:
https://www.cdt.org/policy/cdt-warns-against-widespread-use-domain-name-tactics-enforce-copyright

Links:
[1] http://www.cdt.org/policy/copyright-enforcement-policies-could-have-broad-impact
[2] http://www.cdt.org/files/pdfs/CDT%20Comments%20to%20NTIA%20Copyright%20Task%20Force.pdf

[3] http://cdt.org/files/pdfs/20110216_rogue_sites_statement.pdf
[4] http://cdt.org/files/pdfs/20110314_sohn_testimony.pdf
[5] http://www.cdt.org
[6] http://www.nytimes.com/2010/12/20/business/media/20music.html
[7] http://arstechnica.com/tech-policy/news/2011/02/us-customs-begins-pre-super-bowl-mole-whacking.ars
[8] http://www.cdt.org/blogs/andrew-mcdiarmid/object-lesson-overblocking
[9] http://www.whitehouse.gov/blog/2010/07/22/a-major-milestone-internet-security
[10] http://www.publicknowledge.org/files/docs/COICA_Kaminsky_letter.pdf