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

Statement of the Center for Democracy & Technology

Submitted to the Committee on the Judiciary, United States Senate
Patrick Leahy, Chairman

Regarding the Hearing: "Targeting Websites Dedicated To Stealing American Intellectual Property"

February 16, 2011

The Center for Democracy and Technology (CDT) appreciates the opportunity to submit this written statement for the record of the February 16, 2011 hearing on "Targeting Websites Dedicated to Stealing American Intellectual Property." CDT is a nonprofit public policy organization dedicated to keeping the Internet open, innovative, and free.

CDT supports the goal of reducing copyright and trademark infringement. In particular, we agree that there are websites the main purpose and activity of which is to enable and promote infringement. These sites are true "bad actors" and they deserve to be the target of law enforcement.

CDT has significant concerns, however, about some of the *mechanisms* proposed in the legislation developed by this Committee last year, the Combating Online Infringement and Counterfeits Act (COICA). Specifically, we would urge the Committee to take a hard look at the provisions of COICA that focus on the blocking and seizure of Internet domain names. These domain-name provisions would be almost entirely ineffective at achieving their goal of reducing infringement. At the same time, they would threaten unintended collateral damage in a number of areas, including suppressing lawful speech; exacerbating cybersecurity risks; and encouraging a dangerous jurisdictional scrum in which each country tries to use the domain name system to assert domestic jurisdiction over foreign websites. In short, the bill's domain-name provisions would fail any serious cost-benefit test and simply cannot be justified. The Committee should not proceed with COICA or with legislation proposing similar domain-name focused remedies.

This statement discusses why COICA's domain-name provisions would be ineffective. It then reviews the types of collateral damage that those provisions would risk.

1. Ineffectiveness

The domain-name seizure and blocking contemplated in COICA can be easily circumvented, and thus will have little ultimate effect on online infringement. The domain name system (DNS) performs a relatively simple function: translating text URLs (like www.cdt.org) into machine-readable IP addresses (like 72.32.6.120). Importantly, this function is wholly unrelated to the content available at any given site. Neither seizing nor blocking a website's domain name *removes* the site from the Internet. The servers are still connected and users can still reach the site, including any infringing content.

There are a number of ways a targeted site may still be reached. First, the site's operator could simply register a new domain name for the site. There is ample evidence of just how easy and likely this is in the wake of Immigration and Customs Enforcement's (ICE) seizure of over 100 domain names between June 2010 and February 2011. For example, all of the sports-streaming sites connected to the ten domains seized earlier this month quickly reappeared and are easily located at new domains.

Second, the site's operators could simply publicize its IP address, which users could then bookmark in lieu of saving or remembering the domain name. This is exactly what happened when Wikileaks's DNS service provider terminated the controversial site's account in December 2010; the IP address was immediately and widely available.[1]

Third, 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.

Fourth, in the case of blocking by ISPs, users could easily switch DNS-lookup providers to avoid blocking orders. Since most operating systems come with DNS server functionality built in, savvy users could set up local DNS resolvers on their own computers, thus avoiding any DNS servers that have been ordered to block. In addition, 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. Users who want to engage in infringement will thus easily be able to route their traffic around DNS providers that enforce blocking orders. For users to whom this seems complicated, more sophisticated users may create and distribute software tools to make the process easy.

All of these circumvention techniques are likely to occur as domain-name seizure and blocking become widespread. These sites have a highly motivated and relatively savvy user base, and word will spread quickly as to how best to circumvent any blocking. This means that any impact on infringement from seizing or blocking domain names is likely to be ephemeral at best.

---

[1] 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.

In short, the main impact of COICA's domain-name provisions would be to drive website operators to domains administered by non-U.S. registrars and registries and website users to alternative (but equally easy) Internet navigation methods. The more common the interference with the domain name system, the more the workarounds would become routine The workarounds themselves are trivial and would quickly go viral. Thus, seizing and blocking domain names as contemplated in COICA would be almost entirely ineffective at stopping infringement.

2. Collateral Damage

Interfering with the domain name system in an effort to combat infringement websites would threaten unintended collateral damage in a number of areas.

A. Overbreadth: Impact on Lawful Speech

The version of COICA approved by the Committee last year would affect lawful speech, for several reasons.

First, seizing and blocking domain names each target *entire websites*, which may contain a mix of lawful and unlawful content. This stands in sharp contrast to the notice-and-takedown provisions of the Digital Millennium Copyright Act (DMCA).[2] Under the DMCA process, specific infringing material is identified. That material, and only that material, is then targeted for takedown. Under COICA's domain-name provisions, an enforcement action would affect anything and everything on the website.

The risk of impairing access to lawful content might be mitigated if COICA only targeted pure infringement hubs. In fact, however, the bill has the potential to sweep much more broadly than that. The bill uses the phrase "dedicated to infringing activities," but its definition of that term is broad enough to encompass sites that, far from being "dedicated" to infringement, are actually multipurpose sites featuring a wide variety of content. This is because section 2(a)(1) of the bill includes in the definition any site that is subject to civil forfeiture under 18 U.S.C. § 2323 – which covers any property "used, or intended to be used, in any manner or part to commit or facilitate" criminal copyright infringement. Criminal copyright infringement, defined in 17 U.S.C. § 506, includes any willful infringement committed for financial gain or involving $1,000 worth of goods. So in the end, COICA could be used against any website involved in at least $1,000 worth of infringement, regardless of how much lawful activity also occurs on that site. Measures aimed at such a site's domain name would affect all of that lawful content and speech, not just infringement.

Second, the bill's process for targeting infringing websites does not involve any prior, adversarial hearing. A website can petition to have a court order reversed after-the-fact, but the initial court order to block or seize the domain name occurs without the targeted website having an opportunity to defend itself. Given the one-sided nature of the presentation to the court, with law enforcement making its case unopposed, the risk of mistakes or overaggressive action is high.

[2] 17 U.S.C. § 512 (c)(3).

This risk is evident from news reports about several of the recent domain-name seizures conducted by ICE pursuant to the civil forfeiture provisions of criminal copyright law. Several of the domain names seized in November were for music blogs that contained links to copyrighted songs. The operators of some of those blogs claim that the songs were supplied by the record labels themselves, for promotional purposes.[3] To be clear, CDT expresses no opinion about whether these blogs were authorized to post links to these songs or whether that activity was infringing. But there are significant questions about whether these blogs were such "bad actors" that their entire domain names should be seized. Seizing the domain name affected not just the links to potentially infringing songs, but all of the commentary on the blogs.

In another example, earlier this month ICE seized domain names associated with a Spanish site that had been ruled lawful and non-infringing after extensive litigation in Spain.[4] Again, CDT expresses no opinion about whether the site's activity violates U.S. law. But the outcome in Spain suggests that the site operator, rather than being a clear-cut infringer, might at least have some serious legal arguments that it could offer in its defense. Its domain names were seized nonetheless.

Looking ahead, nothing would prevent COICA's domain-name provisions from being used against user-generated content sites – that is, websites that enable *users* to store, post, and share data. Such sites have many lawful uses, but can in practice be widely used for infringement as well. There is substantial ongoing debate and litigation about whether and when such sites should bear some responsibility and/or liability for infringing activities by users. But at a minimum, that is a question that should be decided only upon a full, adversarial judicial proceeding. By short-circuiting that process, COICA could affect lawful platforms for user speech.

A final reason why COICA's domain-name provisions may affect lawful speech relates to the existence of subdomains. Many web hosting services are constructed in a way such that thousands of individual sites, created and maintained by thousands of individuals, share a single 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. If some infringement sites were hosted on this kind of platform, COICA's domain-name remedies would affect not just the actual offenders, but the *entire platform*. This is because the registrar and registry only have the ability to seize or block the entire domain; they have no ability to take action at the subdomain level. As a result, a great deal of lawful speech could be affected.

In short, COICA's domain-name provisions would impede access to some material that is not itself infringing, but that simply shares a domain name with infringing material.

---

[3] 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; *see also* Mike Masnick, "If Newly Seized Domains Were Purely Dedicated To Infringement, Why Was Kanye West Using One?," *Techdirt*, November 30, 2010, http://www.techdirt.com/articles/20101130/00245312049/if-newly-seized-domains-were-purely-dedicated-to-infringement-why-was-kanye-west-using-one.shtml.

[4] 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.

This overbreadth, in turn, raises serious constitutional questions. There is a strong argument that COICA targets an instrumentality of speech (domain names) and that it creates a prior restraint, effectively trying to censor the owner of a domain name based on his or her illegal activity in the past. Especially given how ineffective COICA's domain-name provisions would likely be in achieving their stated goal, as discussed above, the bill could be vulnerable to a First Amendment challenge.

B. 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.

First, for ISPs, compliance with blocking orders may come at the expense of implementing the DNS Security Extensions (DNSSEC). For over 10 years, Internet engineers have been working to develop and implement a set of standards for addressing security flaws in the domain name system. DNSSEC is finally being deployed; the Office of Science and Technology Policy calls it a "major milestone for Internet security."[5] But having DNS lookup providers either pretend a site does not exist or redirect users 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 a court finding of copyright infringement") 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 drawbacks that providers might prefer to avoid. Congress should avoid steps that would prevent or discourage Internet service providers from implementing this important security standard.

Second, blocking at the service 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 will not switch to other trustworthy U.S.-based DNS providers, but to DNS services located outside of the reach of U.S. law.

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.[6]

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

---

[5] http://www.whitehouse.gov/blog/2010/07/22/a-major-milestone-internet-security.

[6] *See* Letter from DNS security researcher Dan Kaminsky regarding COICA, available at http://www.publicknowledge.org/files/docs/COICA_Kaminsky_letter.pdf.

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, COICA as introduced would create a new and very dangerous opportunity for security risks and crime online.

Finally, encouraging many residential customers to rely on out-of-country DNS servers could undermine the efforts of CDNs (content delivery networks, such as Akamai) to improve the overall speed and efficiency of the Internet as a whole. 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 Maryland 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 infringing 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.

C. International Implications

From an international perspective, Congress should think twice before endorsing domain-name blocking and seizure as common tools for enforcing domestic U.S. law against foreign websites. If other countries were to follow this example, the result would be a dangerous jurisdictional scrum. Other countries, citing the U.S. example, could try to seize or block the domain names of U.S. websites that are lawful here but that violate some foreign law. 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.

To take a concrete example, in 2000, a French court ruled that a Yahoo auction site violated French law because it contained postings for Nazi memorabilia.[7] U.S. courts refused to enforce that judgment, because the site's activity was lawful in the United States. Taking the approach set out in COICA's domain-name provisions, however, in the future a foreign country with a similar complaint could try to seize or block the site's domain name. If the registrar or registry for the domain name in question has an office in that foreign country, it could be ordered to de-register the name.

COICA's domain-name provisions could also serve as precedent for a variety of actions that the United States would characterize 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, and even many liberal

[7] *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.

democracies like Australia and France are considering mandatory regimes in which the government requires ISPs to block certain websites.[8]

Historically, the U.S. State Department has been the strongest global voice against such balkanization of the Internet. Indeed, Secretary of State Clinton has made the concept of a single, global Internet a cornerstone of U.S. foreign policy on Internet matters, as she reaffirmed just yesterday in a major speech.[9] But if the United States sets the precedent that any country can order the blocking of a domain name if some of the content at that name (wherever its physical location) violates the country's local laws, it is hard to see what credibility the United States would have as it urges other countries not to block access wherever they see fit.

To be clear, CDT does not suggest that the United States should not take action against infringement and encourage other countries to do likewise. The concern is simply that, by trying to use domain names as the means for fighting infringement, COICA 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.

In countries where rule of law is weak or entirely absent, that approach would open the door to serious misuse. Once the United States sends the green light, the use of domain-name seizures and blocking to silence other kinds of content considered unlawful in a given country – from criticism of the monarchy in Thailand to any speech that "harms the interests of the nation" in China – would surely spread. In short, the international precedent set by COICA's domain-name provisions would worsen the balkanization of the Internet and undermine the effort to protect the ability of Internet users, human rights defenders, and citizen journalists to speak and access content online.

D. Compliance Costs

Under COICA, law enforcement would issue orders calling on third parties such as registrars, registries, Internet service providers, payment networks, and advertising networks to take action against specific websites. A substantial portion of the costs of the administration of the bill, therefore, would fall on such third parties. While the expense to third parties of complying with COICA is not a primary focus for CDT, the Committee should take account of such costs in conducting a cost-benefit analysis of the tactics proposed in the bill. Given the minimal effectiveness of measures targeting domain names, CDT believes there is little justification for asking Internet service

---

[8] *See* Australian Department of Broadband, Communications, and the Digital Economy, "ISP Filtering," http://www.dbcde.gov.au/funding_and_programs/cybersafety_plan/internet_service_provider_isp_filtering; *see also* Projet de loi d'orientation et de programmation pour la performance de la sécurité intérieure, passed by the French Senate on February 8, 2011 and available at http://www.senat.fr/petite-loi-ameli/2010-2011/262.html (in French; the bill includes a requirement that ISPs block access to Internet sites when ordered by an administrative authority).

[9] Secretary of State Hillary Rodham Clinton, "Internet Rights and Wrongs: Choices & Challenges in a Networked World," Speech at George Washington University, February 15, 2011, http://www.state.gov/secretary/rm/2011/02/156619.htm.

providers, registrars, and registries to bear the cost of carrying out such measures on behalf of law enforcement authorities.

* * * *

CDT does not oppose efforts to fight websites that are truly dedicated to infringing activities. But since domain-name remedies would be ineffective at curbing infringement while carrying a variety of risks and costs, CDT believes it would be a serious mistake for Congress to enact COICA or any legislation similarly focused on using domain names to control infringement. In addition, any measures that aim to sidestep regular judicial process would, at a minimum, need to be much more narrowly tailored than COICA and would require carefully crafted procedural safeguards. In particular, CDT's understanding is that COICA was intended to target sites that have no redeeming qualities, whose whole focus is enabling blatant copyright infringement. As discussed above, however, COICA's definition of "dedicated to infringing activities" reaches much farther than this targeted purpose. COICA likewise envisioned taking strong action against selected websites based on *in rem* proceedings with no adversarial hearing and very little in the way of procedural safeguards to ensure that only true "bad actors" would be affected. For all of these reasons, CDT urges the Committee not to move forward with the approach suggested in COICA.

CDT appreciates the opportunity to offer this statement and stands ready to work with the Committee on this and other important issues of Internet policy. For more information please contact David Sohn, dsohn@cdt.org, or Andrew McDiarmid, andrew@cdt.org.