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 David Sohn
Senior Policy Counsel
Center for Democracy & Technology

Before the House of Representatives Committee on the Judiciary
Subcommittee on Intellectual Property, Competition, and the Internet

Hearing on
"Promoting Investment and Protecting Commerce Online:
Legitimate Sites v. Parasites, Part I"

March 14, 2011

Statement of David Sohn, Center for Democracy & Technology

On behalf of the Center for Democracy & Technology, thank you for the opportunity to participate in this hearing on websites that engage in rampant intellectual property infringement. CDT is a non-profit, public interest organization dedicated to preserving and promoting openness, innovation, and freedom on the decentralized Internet.

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. With respect to the particular focus of this hearing, CDT recognizes that there are websites whose main purpose and activity is to enable and promote infringement. These sites are true "bad actors" and they deserve to be the target of law enforcement.

CDT believes, however, that the specific *means* chosen to address infringement matter a great deal. Some tactics may be attractive from a copyright protection perspective, but would carry significant costs to important values such as innovation and free speech. CDT urges members of this Subcommittee to be aware of this risk and to carefully avoid tactics that would impair lawful Internet-based media and communications tools that are of growing value to consumers, the economy, and society in general.

After a brief note regarding the scope of the problem, this testimony will offer several principles for evaluating proposed policy approaches. It will then address the significant concerns raised by a specific enforcement tactic that has received considerable attention in recent months: the idea of combating allegedly infringing websites by ordering the seizure or blocking of their domain names. In short, CDT believes that legislation targeting domain names would be ineffective at achieving the goal of reducing infringement. At the same time, a domain-name approach would threaten unintended collateral damage in a number of areas, including suppressing lawful speech; exacerbating cybersecurity risks; and encouraging a dangerous global scrum in which each country tries to use the domain name system to assert domestic jurisdiction over foreign websites. Congress should not pursue such an approach.

I. The Problem of Websites Dedicated to Infringement

CDT recognizes the problem of websites that seek to profit by distributing copyrighted material without authorization and without paying the lawful rightsholders. Indeed, CDT has sought to focus attention on websites that masquerade as lawful online music stores when in fact they have not secured any distribution rights. In 2005, CDT filed a complaint at the Federal Trade Commission concerning two websites that charged subscription fees for what they claimed was "100% legal" access to music and video downloads, when in truth the sites merely provided gateways to file-sharing networks on which infringement was common.[1] The FTC filed suit against the operator of one of the

[1] Complaint and request for Investigation, Injunction, and Other Relief before the Federal Trade Commission In the Matter of Mp3DownloadCity.com and MyMusicInc.com, March 8, 2005, http://cdt.org/copyright/20050308complaint.pdf.

sites and ultimately won a court injunction and settlement.[2] In 2007 and 2008, CDT, with the intent of alerting potential users, compiled a "Music Download Warning List" of 47 websites that were falsely posing as legitimate music stores.[3]

Quantifying the problem, however, is exceedingly difficult. Congress should be especially cautious about statistics and studies that purport to measure the problem in dollars and cents. Last year, the General Accounting Office released a report analyzing efforts to quantify the economic effects of counterfeit and pirated goods.[4] GAO found that three widely cited U.S. government estimates of economic losses "cannot be substantiated" and that it "is difficult, if not impossible, to quantify the economy-wide impacts." To be sure, the report observed that research suggests "the problem is sizeable." But methodologies for estimating the economic impact all have limitations, and results are highly sensitive to assumptions.

I would add two additional caveats. First, parties commissioning studies often have vested interests in the results. And second, it is important to remember that the Internet and digital technologies can be highly disruptive of traditional business models for reasons having nothing to do with infringement. For example, the rise of the Internet may have enabled increased infringement of music recordings, but it also has enabled a shift to selling songs individually, new marketplace options like podcasts and music streaming services, and changing patterns in the way people consume and enjoy music. Although these changes may have harmed some incumbent music providers, the changes were the result of innovation and competition. With so much in flux, there is no easy, controlled experiment to isolate the impact of infringement.

Therefore, while there is no question that the infringement problem is real and significant, Congress should not place too much weight on statistics purporting to quantify its overall economic impact. The GAO report suggests that such statistics are generally less than reliable.

II. Principles for Evaluating Policy Approaches to Fighting Infringement

In developing and implementing policies designed to fight infringement-focused websites, CDT believes the Federal Government should take care to observe the following principles.

A. Enforcement efforts should narrowly target true "bad actors." Policies should take care to avoid inadvertent impact on lawful businesses, individuals, and speech.

Enforcement policies should emphasize pursuing and punishing those persons and entities engaged in purposeful, infringing conduct on a substantial scale. Focusing specifically on such "bad actors" avoids inadvertent impact on legitimate business, legitimate free expression, and legitimate technologies.

---

[2] Federal Trade Commission, "File Sharing Operator Settles FTC Charges," Press Release, May 25, 2006, http://www.ftc.gov/opa/2006/05/p2p.shtm.

[3] CDT, "Music Download Warning List," last updated July 2008, http://cdt.org/copyright/warninglist.

[4] General Accounting Office, *Observations on Efforts to Quantify the Economic Effects of Counterfeit and Pirated Goods*, April 2010, http://www.gao.gov/new.items/d10423.pdf.

By contrast, policies that target providers of multipurpose technologies, services, and platforms will risk significant overbreadth. Laws that affect whether and how such platforms operate can carry major consequences for the large body of lawful speech and other activity that the platforms support. Similarly, policymakers should be sensitive to the fact that there are many disputed areas in copyright; mainstream technologies that have been challenged in major copyright litigation over the years include VCRs, mp3 players, printer cartridges, video-sharing websites, online auction sites, and many more.[5] Any new policies aimed at improving enforcement of current law should be designed to target clear-cut cases and should expressly steer clear of legal grey areas.

In addition, policies aimed at "bad actors" should provide sufficient procedural safeguards to protect against the risk of mistakes. The Internet has become a crucial medium for free expression, entitled to the highest level of First Amendment protection.[6] Accidental, overaggressive, or technologically unsophisticated application of tough new policies could impair lawful speech in a variety ways, from stifling individual websites to undermining online platforms that enable speech by users. Providing sufficient due process can help ensure that measures meant for true piracy rings are not brought to bear against the wrong parties. By contrast, policies that would give law enforcement authorities great discretion in a one-sided process create fertile ground for mistakes and inadvertent overbreadth.

B. New policy proposals should be subject to rigorous cost-benefit analysis. There needs to be a sober assessment of both how effective a policy is likely to be and what collateral impact it may cause.

Concern about online infringement is understandably high. But that does not mean that any and all proposals for reducing infringement are worthy of government endorsement. As in any area of policy, proposals for new anti-infringement measures must be subject to rigorous cost-benefit analysis, asking both (i) how effective a proposed policy is likely to be, and (ii) what negative collateral impact it may entail.

Policymakers should be particularly alert to the risk that, where a measure provides benefits to one industry or group and imposes costs on another industry or group, it can be in the interest of the beneficiaries (likely the rightsholders) to lobby strongly even for a measure that offers relatively minor private gains at high social cost. Thus, careful, independent consideration and balancing of the true costs and benefits of suggested measures is essential. If a particular proposal's reduction in online infringement is likely to be of marginal size or fleeting duration (because, for example, it can be easily evaded) and the proposal would impose significant burdens on (for example) legitimate innovators or online free expression, then the proposal should be rejected.

---

[5] For a longer list, *see* CDT, Comments to the Department of Commerce Internet Policy Task Force's Inquiry on Copyright, Creativity, and Innovation in the Internet Economy, November 19, 2010, http://cdt.org/files/pdfs/CDT%20Comments%20to%20NTIA%20Copyright%20Task%20Force.pdf, at 2-4.

[6] *Reno v. American Civil Liberties Union*, 521 U.S. 844 (1997).

C. Addressing foreign infringement activity requires international cooperation.

Where website operators and other participants in online infringement are based outside the United States, unilateral domestic law enforcement tactics will be limited in their effectiveness. Cross-border problems require cross-border solutions.

Cooperating with foreign law enforcement may carry its own challenges. But only cooperative approaches have the potential to stop infringement at its source – to hold wrongdoers personally accountable and to shut down their operations for good. As the recent annual report of the Intellectual Property Enforcement Coordinator observes, "Intellectual property crime knows no borders and effective efforts to combat infringement must involve cooperative law enforcement efforts with foreign governments."[7] The report goes on to detail law enforcement cooperation efforts with Mexico, Latvia, South Korea, and even China. In addition, the final proposed text of the Anti-Counterfeiting Trade Agreement (ACTA) includes a chapter on international cooperation. Congress should not assume that foreign infringement activity is best addressed through additional domestic law.

D. Enforcement alone cannot offer a satisfactory solution to the problem of online infringement.

A full strategy for reducing online infringement requires more than just the "stick" of law enforcement. Just as essential is the "carrot" of compelling legal offerings. One of the best defenses against infringement sites is the continued proliferation of lawful online distribution options that create convenient, easy-to-use ways for consumers to get the content they want in the form that they want it. When consumers have attractive legal options for satisfying their demand, the incentive to rely on illegal sources is greatly reduced.

With this in mind, policymakers should look for ways to encourage the legal marketplace. For example, about five years ago this subcommittee held hearings and debated legislation concerning possible reform and streamlining of the music licensing provisions in Section 115 of the Copyright Act.[8] Ensuring that the structure of current licensing regimes encourages the building of attractive legal services, rather than serving as an obstacle, would help reduce infringement.

Public education is another important and underappreciated component of policy in this area. 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 information-age tools at their disposal. Consumers need to understand that using these tools to engage in infringement is both illegal and wrong. But copyright law can be a highly technical area, and consumers' initial assumptions about what is and is not permitted are often not

---

[7] 2010 U.S. Intellectual Property Enforcement Coordinator Annual Report on Intellectual Property Enforcement, February 2011, www.whitehouse.gov/sites/default/.../IPEC/ipec_annual_report_feb2011.pdf, at 20.

[8] CDT Policy Post, "Music Rights Regime Needs Updating, Should Embrace New Technologies," November 2, 2007, http://cdt.org/policy/music-rights-regime-needs-updating-should-embrace-new-technologies.

accurate. If the goal is to have a long-term impact on the scope of the infringement problem, policymakers should make public education a key part of the discussion.

III. Policy Concerns with Tactics that Target Domain Names

In recent months, there has been considerable focus on using the domain name system (DNS) to go after websites associated with infringement. Since late June 2010, Immigration and Customs Enforcement (ICE) and the Department of Justice have executed seizure warrants for over 100 domains as part of "Operation In Our Sites."[9] S. 3804, the "Combating Online Infringement and Counterfeits Act" from the 111th Congress, would have expanded the practice of such seizures, giving the Attorney General the ability to bring *in rem* actions against both domestic and foreign domain names and to compel intermediaries, including Internet service providers (ISPs), to seize or block the domain.[10]

CDT has significant concerns about both the low effectiveness and the high collateral impacts of this approach to fighting infringement. In light of these concerns, we believe that a policy that codifies and encourages large-scale reliance on domain names as an enforcement mechanism would fail any cost-benefit test. For the reasons set out below, we would strongly urge Congress not to proceed with legislation proposing domain-name focused remedies.

A. Ineffectiveness

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) into machine-readable IP addresses (like 72.32.6.120). This function is wholly unrelated to the content available at any given site. Importantly, 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. This is both easy and likely. 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.

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 the provider of Wikileaks's DNS service provider terminated the

[9] 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.

[10] Combating Online Infringement and Counterfeits Act, S. 3804, 111th Congress (2010).

controversial site's account in December 2010; the IP address was immediately and widely available.[11]

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, 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. This means that any impact on infringement from seizing or blocking domain names is likely to be ephemeral at best.

In short, the main impact of domain-name seizure and blocking 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, rendering the domain-name approach almost entirely ineffective.

B. Overbreadth: impact on lawful speech

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

First, these methods target *entire domains*, which may contain a mix of lawful and unlawful content, including non-Web content like email or instant messaging connections. This stands in sharp contrast to the notice-and-takedown provisions of the DMCA. Under the DMCA process, specific infringing material is identified. That material, and *only* that material, is then targeted for takedown. Enforcement actions targeting a domain name itself would not be so narrowly targeted; they would affect anything and everything associated with that domain.

[11] 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.

The risk of impairing access to lawful content might be mitigated if there were strong guarantees that only pure infringement hubs would be targeted. For that purpose, a tightly focused definition of the "bad actor" websites would be essential. Last year's Senate bill, S.3804, failed to ensure such a narrow focus. Although that bill used the well-intended phrase "dedicated to infringing activities," its definition of that term was broad enough to encompass sites that, far from being "dedicated" to infringement, are actually multipurpose sites featuring a wide variety of content.

The risk of sweeping in non-infringing content is exacerbated if seizure or blocking orders are issued without a full adversarial hearing. When law enforcement makes its case unopposed and a domain name owner has no opportunity to defend itself, mitigating factors and overbreadth issues may not come to light before the name is seized or blocked. In a one-sided process, the risk of mistakes or overaggressive action is high.

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 which 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.[12] 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, and it seems under ICE's seizure process these questions were not fully considered. In addition, seizing the domain name affected not just the links to potentially infringing songs, but all of the commentary on the blogs.

In another example, in February ICE seized domain names associated with a Spanish site that had been ruled lawful and non-infringing after extensive litigation in Spain.[13] 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. The end result was that a domain that Spanish courts had declared to be lawful was seized by the U.S. Government.

Under a flawed definition or one-sided process, little would prevent domain-name seizure or blocking from being used against user-generated content sites – that is, websites that enable *users* to store, post, and share data. This is especially true in the case of lesser-known sites that officials may not be familiar with. A judge might think

---

[12] 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.

[13] 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.

twice before issuing an order against a well-known platform, but not its equally legitimate start-up competitor. 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. Short-circuiting that process would risk affecting lawful platforms for user speech.

A final reason why domain-name seizure and blocking 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, domain-name seizure or blocking would affect not just the actual offenders, but the *entire platform*. Moreover, the existence of additional subdomains and thus the overbroad impact might not be immediately apparent to law enforcement authorities looking at a particular infringement website. As a result, a great deal of lawful speech could be affected.

Again, the recent ICE seizures provide a cautionary tale. In early February, ICE executed seizure of ten domain names linked to sites allegedly hosting child pornography. Child pornography is a despicable crime. But in seizing one domain, "mooo.com," ICE inadvertently blocked thousands of innocent and unrelated subdomains.[14] 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 an ICE banner announcing that the domain had been seized for violating child pornography laws.

Websites hosted at those subdomains include many personal websites that do not appear to be hosting any illegal content. In looking into the incident, CDT discovered personal blogs, discussion forums, a small business, and sites where academic researchers shared papers and professional information.[15] During the time all mooo.com subdomains were inaccessible, these users were no doubt shocked to see as they tried to visit their sites not only that their sites were inaccessible, but that law enforcement was telling other would-be visitors that the sites had been taken down due to child pornography. This is an incredibly serious allegation that alone can damage an individual's reputation.

The experience of mooo.com users stands out as the most egregious example to date of overblocking that can result from domain-name seizure. Clearly ICE had not thoroughly

[14] 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.

[15] *See, e.g.,* http://greyghost.mooo.com/; http://cowbell.mooo.com/catalog/index.php.

ensured that the action it was taking was narrowly tailored to the criminal actors, and the result silenced protected speech and harmed the reputations of innocent parties.

The risk of overbreadth would be greatly exacerbated if legislation in this area were to include a private right of action. As noted above,[16] there is a long history of civil copyright challenges to mainstream technologies and bona fide businesses. Narrowly targeting a new enforcement tactic at true "bad actors" would be impossible if any private rightsholder could initiate an action. Borderline cases inevitably would be initiated and the unintended impact on lawful businesses and speech would be significant. Adding a private right of action to the kind of process contemplated last year's Senate bill would intensify that tactic's risks and costs.

In sum, seizing and blocking domain names would impede access to some material that is not itself infringing, but that simply shares a domain name with infringing material. This overbreadth, in turn, raises serious constitutional questions. There is a strong argument that the tactic of domain name seizure and blocking 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 domain-name focused enforcement measures are likely be in achieving their stated goal, as discussed above, a bill that adopts the approach could be vulnerable to a First Amendment challenge.

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.

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."[17] 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 performance 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.

---

[16] *See supra* note 5 and accompanying text.

[17] Andrew McLaughlin, "A Major Milestone for Internet Security," White House Office of Science and Technology Policy Blog, July 22, 2010, http://www.whitehouse.gov/blog/2010/07/22/a-major-milestone-internet-security.

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.[18]

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 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.

D. 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 are asserted to 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

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

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 (located at the Yahoo.com domain) violated French law because it contained postings for Nazi memorabilia.[19] 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 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 transfer control of the name.

Enshrining domain-name seizure and blocking in statute 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 democracies like Australia and France are considering mandatory regimes in which the government requires ISPs to block certain websites.[20]

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 in a major speech last month.[21] But 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 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 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.

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 attempt to silence other kinds of content

---

[19] *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.

[20] *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 (France), 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: bill including a requirement that ISPs block access to Internet sites when ordered by an administrative authority).

[21] 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.

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 codification or expansion of domain-name focused enforcement efforts 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.

E. Compliance costs

A substantial portion of the costs of domain-name-focused enforcement measures would fall on third parties – specifically, registrars, registries, or ISPs. While the expense to third parties of complying with seizure and blocking orders is not a primary focus for CDT, Congress should take account of such costs in conducting a cost-benefit analysis of such tactics. Given the minimal effectiveness of measures targeting domain names, CDT believes there is little justification for asking registrars, registries and ISPs to bear the cost of carrying out such measures on behalf of law enforcement authorities.

IV. Conclusion

Fighting online infringement is a worthy goal. The tactics policymakers choose, however, matter a great deal. Unfortunately, there is no "silver bullet" that can eliminate infringement sites entirely or make them inaccessible to Internet users. Domain-name blocking and seizures are certainly not the answer; codification and widespread use of this tactic would carry costs and risks that would far exceed its minimal impact on infringement. CDT believes it would be a serious mistake for Congress to enact legislation focused on using domain names to control infringement.

As the principles discussed above suggest, a sound policy approach regarding enforcement in this area would 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. Moreover, a recent study found that a small group of users (around 100) were responsible for the lion's share of infringing files on major BitTorrent sites.[22] This suggests that well-targeted enforcement cases could have a substantial impact and be well worth the effort.

To the extent Congress believes new enforcement tools are necessary, it should look for remedies other than domain-name blocking and seizures. Cutting off infringers' sources of financial support would be one area to explore. In addition, Congress should be careful to focus any special new enforcement mechanisms narrowly on cases in which it has been shown that current tools cannot work. Congress should take into account not

[22] Ruben Cuevas *et. al.*, *Is Content Publishing in BitTorrent Altruistic of Profit-Driven?*, ACM CoNEXT Conference (November 30 – December 3, 2010, Philadelphia, PA), http://conferences.sigcomm.org/co-next/2010/CoNEXT_papers/11-Cuevas.pdf. *See also* Carlos III University of Madrid, "A research study identifies who uploads the majority of the content to the P2P piracy networks," Press Release, http://www.uc3m.es/portal/page/portal/actualidad_cientifica/noticias/P2P_network (last visited March 7, 2011).

just existing legal mechanisms, but other available tools as well. For example, major payment systems have established procedures that can be used to cut off payments to infringement sites. A representative from Visa recently told a Senate Committee that "few intellectual property owners have availed themselves of Visa's procedures" and that "[o]ther payment systems have shared similar experiences."[23] It is unclear why this potentially powerful tool is not being used more widely by rightsholders.

Finally, any enforcement measures that aim to sidestep normal judicial process would, at a minimum, need to be narrowly tailored and contain carefully crafted procedural safeguards. Without such safeguards, there would be a risk of impairing lawful websites and speech, as the experience with ICE seizures has already begun to demonstrate.

CDT appreciates the opportunity to testify today and stands ready to work with the Subcommittee on this and other important issues of Internet policy.

[23] *Hearing on Targeting Websites Dedicated to Stealing American Intellectual Property Before the Senate Comm. on the Judiciary*, 112th Cong. (February 16, 2011) (statement of Denise Yee, Visa, Inc.) at 15.