Editors: Patrick McDaniel, mcdaniel@cse.psu.edu
Sean W. Smith, sws@cs.dartmouth.edu

Exposing the Flaws of Censorship by Domain Name

Wendy Seltzer
Fellow, Princeton Center for Information Technology Policy

Imagine if online map providers were ordered to block the street location of Fake Flicks and Footwear, a bricks-and-mortar store unabashedly dedicated to infringing activities (selling copied DVDs and counterfeit designer boots). The incomplete map, with a gap where the 3Fs shop once stood, might stymie a few would-be buyers of fake UGG boots, but it could also interfere with many unrelated lawful activities. It might divert friends using the shop as a waypoint ("meet me at the coffee shop across the street from 3Fs"), investigators from a smaller label trying to trace counterfeits of their brand, or even a fire truck responding to an emergency call. Meanwhile, the regular customers (and those still using paper maps) would have no trouble finding their way to the store.

A similar combination of confusion and inefficacy would result if Congress passes the Combating Online Infringement and Counterfeits Act (COICA), introduced in September 2010.[1] The bill would force operators of Domain Name System (DNS) components and Internet service providers to block the resolution of domain names "dedicated to infringing activities," thereby harnessing remote technical connections to censor online content. The bill's DNS-based mechanisms for censoring access to Internet sites could squelch free expression and weaken the Internet infrastructure without substantially reducing infringement and counterfeiting. The proposal and its flaws emphasize the challenges in considering the system-wide effects of a seemingly limited intervention. Securing an entire system requires us to take a global view, watching for direct and indirect effects—including the likely impact of human responses.

A Flawed Proposal

Senators Patrick Leahy (D-Vt.) and Orrin Hatch (R-Utah) introduced COICA last fall in the US Senate, where it was referred to the Senate Judiciary Committee. It was quickly updated by a "manager's amendment," which removed its craziest feature—a publicly contributed blacklist of alleged infringing sites—and exempted authoritative domain name servers, but maintained the bill's basic structure. The proposal drew opposition from numerous groups and individuals, including technology experts, law professors, human rights and civil liberties organizations, and Internet companies. The Recording Industry Association of America, the Motion Picture Association of America, and many sports leagues and luxury brands voiced support. In November, the Judiciary Committee unanimously approved the bill (S. 3804),[2] sending it to the full Senate. There, Senator Ron Wyden (D-Ore.) has threatened to block the bill, saying, "Deploying this statute to combat online copyright and infringement seems almost like a bunker buster cluster bomb when really what you need is a precision-guided missile."[3]

COICA proposes using the Internet's DNS as a chokepoint, authorizing the Attorney General to take *in rem* action for an injunction against "any domain name… used by Internet sites dedicated to infringing activities."[1] The bill would give the Attorney General the power to blacklist domain names of sites "offering or providing access to [unauthorized copyrighted works] in complete or substantially complete form, by any means, including by means of download, transmission, or otherwise, including the provision of a link or aggregated links to other sites or Internet resources for obtaining such copies for accessing such performance or displays." The Attorney General could also blacklist sites offering items with counterfeit trademarks.

COICA applies different blocking mechanisms, depending on where the domain's components are located. If either the registry or registrar for the domain name is in the US, that registry or registrar will be ordered to "suspend operation of… the domain name." If neither the registry nor registrar is in the

1540-7993/11/$26.00 © 2011 IEEE

US, then US companies even more remote from the alleged infringing activity—Internet service providers, financial transaction providers, and advertising networks—would be pressed into blocking service. In particular, service providers offering DNS would be ordered to "take technically feasible and reasonable steps designed to prevent a domain name from resolving to that domain name's Internet protocol address." (The location of the domain name's registered owner is irrelevant to the COICA-ordered blocking, which a judge can issue at the Attorney General's request if any Internet site using the domain "conducts business directed to residents of the United States.")

Seemingly to show its existing power over domains registered with US-based registries, Immigration and Customs Enforcement (ICE) announced on 29 November 2010 the seizure of 82 domain names in the .com and .net registries allegedly "involved in selling counterfeit goods."[4] The sites previously operating at those domains were replaced with the following alert: "This domain name has been seized by ICE—Homeland Security Investigations." Many of the site names suggested physical goods (such as burberryoutletshop.com and nfljerseysupply.com), but others mixed commentary and music promotion or search (including dajaz1.com and torrent-finder.com). The Egyptian owner of torrent-finder.com is fighting the seizure, saying his site was a news and search aggregator, not a piracy haven, while the owner of dajaz1.com asserts he was sent tracks for posting by record labels and artists' representatives.

If enacted, COICA threatens free expression online and the integrity of the Internet's DNS. It will also undermine US foreign policy, contradicting the State Department's strong support of Internet freedom abroad.

Restricting Free Speech

The First Amendment of the US Constitution establishes strong safeguards against government restrictions on speech, to protect both the speaker and listener. Yet, COICA would operate as the most disfavored type of speech restriction—prior restraint, stopping speech before the site operator has a meaningful chance to be heard in its defense. Particularly for operators outside the US, their first notice of action might be seeing that the domain name fails to resolve, leaving them to challenge the takedown only after the fact.

Domain name blocking is a crude mechanism for addressing infringement, and the procedures specified in COICA increase the likelihood of erroneous over-blocking. COICA targets "Internet sites" but authorizes action against a domain *used* by an Internet site—although the domain name could be hosting much more than a single site, and a site could host a variety of material. Without adequate opportunity for the domain owner to challenge beforehand, this blocking leaves too much room for erroneous or even malicious takedown. Claims of "infringing activity" could be used pretextually to block access to political critics—as in Russia, where the police asserted copyright enforcement when they raided an environmental group and confiscated computers containing allegedly pirated Microsoft software.[5] (Microsoft has subsequently granted a blanket license to such groups.)

It's particularly unfortunate to see the proposed use of domain names for censorship so soon after Secretary of State Hilary Clinton promoted Internet freedom as a key plank of the State Department's work.[6] If, as Clinton stated, "we stand for a single Internet where all of humanity has equal access to knowledge and ideas," we should set an example through our own laws and practices. Instead, COICA-mandated blocking looks like that conducted by restrictive regimes such as China, where the "Great Firewall" tampers with the DNS resolution of unwanted sites, including those of foreign news organizations, human rights organizations, and local groups identified as dissidents such as Falun Gong. (The Chinese firewall supplements DNS tampering with IP blocking and keyword-based TCP resets, preventing online discussion of issues the government deems sensitive. See http://opennet.net/research/profiles/china for more information.)

Due process of law generally requires that a person accused of wrongdoing be given notice of the allegations and an opportunity to be heard before being punished. COICA inverts that sequence.

Impeding Due Process

Due process of law generally requires that a person accused of wrongdoing be given notice of the allegations and an opportunity to be heard before being punished. COICA inverts that sequence: the domain name registrant won't necessarily be heard before an order blocking his domain issues; he's only offered service of process by mail, email, and publication. This abbreviated process increases the risk of error. The party who best knows the uses of the domain name—and whether sites' uses of copyrights or trademarks were authorized—will not be present to offer the court those explanations.

COICA would impose a radical extension of indirect liability for copyright and trademark infringement. Traditional liability begins with the direct infringer, the one making unauthorized reproductions of copyrighted works or counterfeiting trademarked goods. Direct liability specifically targets the unlawful activity and pressures the responsible entity.

Secondary liability is more remote, stretching the connection between harm and liability. The Napster file-sharing service wasn't accused of copying music directly. However, it was held liable for providing software that assisted users' copyright infringement and for maintaining a directory of infringing music files. Grokster, which had decentralized its network further, was found to "induce" infringement. In those cases, the defendants were found liable for facilitating specific infringements or building systems intentionally directed at infringing uses. Already, the indirection takes its toll, however, as the systems' noninfringing uses were shut out as well.

COICA's orders would impose a liability even more remote from the underlying infringement. The service providers COICA targets have no participation in infringement or intent to induce it, so we would have no grounds for holding general-purpose DNS resolvers liable under traditional doctrine.

The shift hurts due process for the site, service providers, and users. Service providers have less direct incentive than their customers to defend customers' speech, particularly at the level of a registry or registrar earning less than US$10 a year for a domain name. Hence elsewhere in the US Code, law protects Internet service providers from liability or provides safe harbors for their carriage of users' speech, leaving the disputes to their proper parties—the actor and the person complaining about the actions.[7,8] That split correctly mirrors the architectural layering of the Internet: content disputes belong at the content layer, not at the lower protocol layer, where COICA misuses protocol elements as chokepoints.

Interfering with Technical Architecture

Furthermore, COICA interferes with the technical architecture of domain name resolution, undermining the reliability of US-based participants and DNS consistency. DNS offers a distributed, hierarchically rooted directory for matching names to IP addresses. DNS Security Extensions (DNSSEC) provides cryptographic assurance of the integrity and authenticity of these lookups. The existing DNS promotes consistency—from wherever you access a domain name, it will point to the same resource (or at least one under control of the domain owner—for example, using DNS for simple load-balancing). DNS-based blocking weakens this assertion, even as DNSSEC offers the promise of more-trusted lookups.

If the US asserts control over remote activity through US-based registries and registrars, domain registrants looking for security could be driven away from using these registries (including .com, .net, and .org registries). Even based abroad, they could have their access disrupted from US-based Internet connections using US-controlled DNS. Of course, technically sophisticated users could quickly find alternate DNS providers, most simply by pointing to DNS resolvers outside the US. But the blow to DNS consistency, decreasing the universality of Uniform Resource Locators, remains.

Moreover, legal challenges to

the DNS infrastructure might prompt further decentralization, just as challenges to centralized file-sharing prompted ever-more-distributed peer-to-peer applications. The discussion around ICE's seizures and DNS challenges to Wikileaks.org have spurred calls for alternate and peer-to-peer DNS (enacting John Gilmore's adage, that "the Net interprets censorship as damage and routes around it"). I generally appreciate decentralization and agree even here it might be helpful, but fragmented DNS could also reduce assurances of name uniqueness and universal, uniform resolution.

Introducing Blocking-Induced Errors

In addition to the concerns already mentioned, COICA could also induce new errors unrelated to the search for infringing materials. DNS is agnostic to its uses. While COICA assumes that domain names are used for websites and directed toward infringing activity, a DNS server doesn't know why a user is requesting domain name lookup: the user could be trying to locate a website, identify the sender of an email message, ascertain whether a user is authorized to access system resources, or analyze server log files. Indeed, because of this generality, the DNS protocol has been used for other lookups, such as querying spam blacklists.

As service providers move to comply with court-ordered blocking, their systems will likely respond differently to requests for enjoined names (particularly as they're required to take "technically feasible and reasonable steps" to prevent a domain name from resolving, without being required to modify their networks). If they do anything at all, then, providers might be forced to cobble solutions onto existing networks. Without a standard "this domain exists, but its name records can't be shown," DNS providers may synthesize substitute responses, send the no-such-domain response (NXDOMAIN), or fail to respond when asked for information about a blocked domain. Thus look-ups for the same name may return different results from different network locations. Unpredictable errors are even more difficult to debug.

Divergent responses might interfere with a range of Internet-connected systems, introducing errors similar to those reported in 2003, when Verisign, the .com and .net registry, introduced "Sitefinder," a wildcard response to look-ups for nonexistent domains.[9,10] Sitefinder offered a browser-based search page (with advertising revenue possibilities for Verisign) in response to a DNS look-up for a nonexistent domain. Some Web users objected to the search page (as did providers who had previously offered their own searches); other objections showed the range of unintended consequences to protocol-tampering. Sitefinder interfered with automated link checkers and spam filters checking for a NXDOMAIN response, increased traffic, and prompted workarounds that introduced new bugs. The Internet Corporation for Assigned Names and Numbers (ICANN)'s Security and Stability Advisory Committee identified further concerns for Internet telephony, email, internal error-checking, and security management.[11] In response to "clear and significant danger to the security and stability of the domain name system," ICANN now prohibits synthesized responses in new generic top-level domains.

COICA's assumptions about the use of DNS, then, increase the fragility of both DNS and the Internet services that depend upon it.

Intellectual property protection must be balanced with protection for free expression, due process, and technical flexibility. More direct legal means already exist to punish infringement and cut off access to infringing activity; a domain name can be taken or transferred after an adversarial hearing or even a UDRP proceeding (a rapid dispute-resolution process in which the domain owner can reply to complaints of bad-faith registration or use). There, domain seizure comes at the end of the process, not its beginning.

Thanks to its architectural design for openness and interoperability, the Internet has supported a wealth of creative expression, communication, and technological innovation. The centrally rooted DNS has helped enable interconnection for the distributed network. By cutting at that root, COICA threatens the stability of the Internet expression built around it. Legislation that respects the Internet's layered architecture would protect legal rights more effectively with fewer unintended consequences. □

References

1. "Combating Online Infringement and Counterfeits Act," US Senate, Bill S. 3804, 20 Sept. 2010; www.govtrack.us/congress/billtext.xpd?bill=s111-3804.
2. "Senate Judiciary Committee Advances Bipartisan Bill to Combat Copyright Infringement and Counterfeits," press release for Senator Patrick Leahy, 18 Nov. 2010; http://leahy.senate.gov/press/press_releases/release/?id=45b5a544-0f49-46d8-9782-ab7a3fe43a1f.
3. J. Gruenwald, "Wyden Threatens to Block Online IP Bill," *National J.*, 18 Nov. 2010; http://techdailydose.nationaljournal.com/2010/11/wyden-threatens-to-block-onlin.php.
4. "ICE Seizes 82 Website Do-

mains Involved in Selling Counterfeit Goods as Part of Cyber Monday Crackdown," US Immigration and Customs Enforcement, 29 Nov. 2010; www.ice.gov/news/releases/1011/101129washington.htm.

5. C.J. Levy, "Russia Uses Microsoft to Suppress Dissent," *New York Times*, 11 Sept. 2010; https://www.nytimes.com/2010/09/12/world/europe/12raids.html&pagewanted=all.
6. H.R. Clinton, "Remarks on Internet Freedom," 21 Jan. 2010; www.state.gov/secretary/rm/2010/01/135519.htm.
7. "Communications Decency Act," The Code of Laws of the United States of America (U.S.C), title 47, section 230.
8. "Digital Millennium Copyright Act," The Code of Laws of the United States of America (U.S.C), title 17, section 512.
9. "IAB Commentary: Architectural Concerns on the Use of DNS Wildcards," Internet Architecture Board, 19 Sept. 2003; www.iab.org/documents/docs/2003-09-20-dns-wildcards.html.
10. "SAC 032 Preliminary Report on DNS Response Modification," ICANN Security and Stability Advisory Committee, June 2008; www.icann.org/en/committees/security/sac032.pdf.
11. "SAC041: Recommendation to Prohibit Use of Redirection and Synthesized Responses by New TLDs," ICANN Security and Stability Advisory Committee, 10 June 2009; www.icann.org/en/committees/security/sac041.pdf.

***Wendy Seltzer** is founder of Chilling Effects Clearinghouse, which tracks legal threats to online expression (http://chillingeffects.org). Her research interests include privacy, digital copyright, and open innovation. Seltzer has a JD from Harvard Law School. She's a Fellow of the Princeton Center for Information Technology Policy and of the Berkman Center for Internet & Society at Harvard University. Contact her at wendy@seltzer.org.*

Selected CS articles and columns are also available for free at http://ComputingNow.computer.org.