Computer & Communications Industry Association

*Before the*

Senate Judiciary Committee

*Regarding*

"Targeting Websites Dedicated To Stealing American Intellectual Property"

February 16, 2011

**Statement of Edward J. Black**

President and CEO Computer & Communications Industry Association

---

On behalf of the Computer & Communications Industry Association, I appreciate the committee's consideration of this testimony on the matter of seizing domain names associated with infringing activities online. This written testimony addresses the general issue of seizing domain names, and then focuses on the last legislative incarnation of that policy, S. 3804. It identifies risks related with domain name seizure and cautions against adopting S. 3804 in any form, as the bill would not only prove ineffective but also endanger cybersecurity. The Computer & Communications Industry Association joins with prominent Internet engineers,[1] human rights advocates,[2] law professors,[3] educational groups,[4] and other technology organizations[5] in opposing S. 3804.

---

[1] *See* Letter from 89 Internet engineers to the members of the Senate Judiciary Committee, *available at* <http://www.publicknowledge.org/files/docs/COICA_internet_engineers_letter.pdf>; Dan Kaminsky, *DNS Filtering and S.3804, 'Countering Online Infringement and Counterfeiting Act'* (Oct. 2010), *available at* <http://www.publicknowledge.org/files/docs/COICA_Kaminsky_letter.pdf>.

[2] *See* Letter from American Civil Liberties Union, Center for Democracy & Technology, Electronic Frontier Foundation, Freedom House, Human Rights First, Human Rights Watch, Rebecca MacKinnon, Reporters Sans Frontières, and World Press Freedom Committee to Chairman Patrick J. Leahy and Ranking Member Jeff Sessions, United States Senate (Oct. 26, 2010), *available at* <http://www.publicknowledge.org/files/docs/COICA_human_rights_letter_0.pdf>.

[3] *See* Letter from 49 law professors to the Senate Judiciary Committee (Nov. 16, 2010), *available at* <http://www.publicknowledge.org/files/docs/LawProfCOICA.pdf>.

[4] *See* Letter from Gregory A. Jackson, Vice President for Policy & Analysis, Educause, to Chairman Patrick J. Leahy and Ranking Member Jeff Sessions, United States Senate (Sep. 27, 2010), *available at* <http://www.publicknowledge.org/files/docs/COICA_EDUCAUSE_letter.pdf>; Letter from Cameron P. Wilson, Director of Public Policy, Association for Computing Machinery, to Chairman Patrick J. Leahy and Ranking Member Jeff Sessions, United States Senate (Sep. 28, 2010), *available at* <http://www.publicknowledge.org/files/docs/COICA_USACM_Letter.pdf>.

[5] *See* Letter from American Association of Law Libraries, American Library Association, Association of College and Research Libraries, Association of Research Libraries, Center for Democracy and Technology, Computer and Communications Industry Association, Consumer Electronics Association, Electronic Frontier Foundation, Home Recording Rights Coalition, NetCoalition, and Public Knowledge to Chairman Patrick J. Leahy and Ranking Member Jeff Sessions, United States Senate (Sep. 27 2010), *available at* <http://www.publicknowledge.org/files/docs/JointLetterCOICA.pdf>; Letter from Markham C. Erickson, Executive Director, NetCoalition, to The Honorable Patrick Leahy, Chairman, Senate Committee on the Judiciary (Nov. 15 2010), *available at* <http://www.publicknowledge.org/files/docs/COICA_NetCoalition_letter.pdf>.

## I. Summary

This written testimony argues that attacking allegedly unlawful content at the architectural layer of the Internet is a dangerous precedent to set, one which will further empower oppressive and authoritarian regimes to the political and economic detriment of the United States. Moreover, such a strategy is likely to prove ineffective and is already yielding false positives. This testimony also argues that much of S.3804, the Combating Online Infringement and Counterfeiting Act ("COICA"), represents dangerous and unworkable responses to the problem of infringement. Not only is COICA unlikely to remedy the problem of foreign infringement, but it also threatens cybersecurity and is overbroad in its sweeping coverage of domestic sites and lawful products and services. In addition, COICA will further embolden authoritarian governments abroad, and lacks traditional safeguards to prevent its abuse at home. The solution to addressing infringement abroad is to persuade our trading partners to enforce the intellectual property laws that they have enacted – an objective in which we have already invested considerable political capital.

## II. Seizing Domain Names

The Internet is an amazing tool for global e-commerce that has opened up many new markets to U.S. firms. It also resembles a giant copying machine which resists control by any one person, company or government. The result is that, in addition to adding $2 trillion to annual U.S. GDP,[6] the Internet upsets old business models – for better or worse – and occasionally complicates the enforcement of intellectual property rights online.

Over the past year, domain name seizures have figured prominently in the online enforcement effort. This conversation has largely ignored the reality that, as Secretary Clinton stated only yesterday, "walls that block the Internet… are far easier to erect than to maintain." The challenges of using Internet architecture to police content has not stopped numerous governments, authoritarian and democratic, from trying to restrict Internet freedom. As a general rule, it is antithetical to the economic interests of the United States to validate the strategy of regulating Internet architecture to police content. As recent events have demonstrated, authoritarian governments cannot stand the openness and democratic nature of the Internet, and

[6] According to the National Economic Council this yields over $6,500 per person. Exec. Ofc. of the President, Nat'l Econ. Council/OSTP, *A Strategy for American Innovation: Driving Towards Sustainable Growth and Quality Jobs*, Sept. 2009, at 5, *available at* <http://www.whitehouse.gov/administration/eop/nec/StrategyforAmericanInnovation>.

seek any excuse to regulate it. Even democratic governments occasionally feel the temptation to control the Internet, and it is of paramount importance that the United States lead by example.

Nevertheless, under a very narrow set of circumstances, the extreme approach of attacking unlawful activity at the architectural layer of the Internet may be a necessary option of last resort. However, as evidenced by mistakes already made, domain name seizure must be exercised carefully. As a broad enforcement tool, domain name seizure is in many cases unwise and unwieldy.

With respect to infringers located inside the United States or otherwise within the reach of U.S. law enforcement, a domain name seizure may be followed by arrest and prosecution. Domain name seizure thus serves to cease immediate infringing activity, but only as an initial approach to a more traditional law enforcement approach. If a domain name seizure is not followed by an arrest, most infringers easily re-register their domains. Aside from yielding more fees for domain name registrars, this exercise results in little effect.

Because infringers overseas are not being arrested concurrently with the domain name seizure, they generally re-register with immunity. For example, in June 2010 nine domain names were seized by the United States Immigration and Customs Enforcement Agency ("ICE") under the banner of a new initiative called "Operation In Our Sites."[7] Only a few days after the seizure and initiative were announced on a lot at Walt Disney Studios in Burbank, CA, at least two of the seized domains were back online under different domain addresses.[8] After ICE shut down the tvshack.net domain of Swedish company TV Shack, the site's operators relaunched at tvshack.cc, a domain administered by the Australian territory of the Cocos Islands. When the .cc domain was seized, sites appeared at tvshack.bz and tvshack.org.uk. Additionally, the seized Movie-Links.tv site appeared back online at its new www.watch-tv-movies.info address.

In addition to the ease with which infringers re-register, several mistakes have been made. For instance, ICE seized several sports-streaming sites just before the Super Bowl, including Spanish website Rojadirecta.[9] Rojadirecta is of special note because ICE's seizure comes after, and despite, Spain's determination that the site is legal.[10] Thus, ICE's actions as to

[7] Michael Cieply, "9 Domain Names Seized in Fight Against Internet Theft," Media Decoder Blog, *N.Y. Times* (June 30, 2010), *available at* <http://mediadecoder.blogs.nytimes.com/2010/06/30/in-anti-theft-effort-officials-seize-9-domain-names>.

[8] Erick Schonfeld, "TV Shack Flouts the Feds by Moving Video Piracy Site to Offshore Domain," *TechCrunch* (Jul. 6, 2010), *available at* <http://techcrunch.com/2010/07/06/tv-shack-piracy>.

[9] Bianca Bosker, "Rojadirecta.org One of Several Sites SEIZED by U.S. Authorities," *The Huffington Post* (Feb. 2, 2011), *available at* <http://www.huffingtonpost.com/2011/02/02/rojadirecta-org-seized_n_817458.html>.

[10] *Id. See also* Letter from Senator Ron Wyden to The Honorable John Morton, Director, U.S. Immigration and Customs Enforcement 2 (Feb. 2, 2011), *available at* <http://www.scribd.com/doc/48143849/Wyden-Ice-Letter-to-Holder-and-Morton>.

Rojadirecta are particularly troubling in their complete disregard of another country's sovereign determination of legality. Even assuming that Rojadirecta were a clearly illegal site, the efficacy of seizing rojadirecta.com is dubious at best. After the seizure of the .com domain, users began using rojadirecta.es, as the U.S. Government has no control over .es, the Spanish ccTLD. Internet traffic statistics from Alexa Internet, Inc. suggest that rojadirecta.es is now receiving *more* daily traffic than rojadirecta.com was receiving prior to seizure. This is hardly cause for declaring victory.

For another troubling example, one need look no further than the November 2010 seizure of hip hop blogs OnSmash and RapGodFathers.[11] The seizure of these blogs illustrate the tensions between a common marketing technique in the music industry called "leaking", where labels, agents, or artists themselves send popular websites new songs and videos to post in order to garner attention, and the immediate sanctions implemented through ICE's "Operation In Our Sites" initiative.[12] Similarly, in his recent letter to ICE Director John Morton, Senator Ron Wyden (D-OR) called into question the November seizure of dajaz1.com based on an ICE special agent's ability to download four songs that were legally provided to dajaz1.com's operator for purposes of distribution.[13]

Domain name seizure therefore seems unwise in many circumstances. It has the unfortunate result of implying that international IP norms are impotent, as well as highlighting the apparent control of the U.S. Government over Internet architecture. This is occurring at a time when various governments are proposing to transfer Internet governance functions to a United Nations entity, in the hopes of exerting more control over Internet governance. Furnishing more arguments for that troublesome campaign, particularly when the law enforcement gains are dubious, is imprudent.

Finally, domain name seizure is a blunt instrument. While in some cases, all of the content of a site will be infringing, in many cases this will not be the case. As mentioned in the cases of OnSmash and RapGodFathers above, songs and videos will often be given to the website by the artist herself, her agent, or even the label. Such "leaking" of new and upcoming material is a common marketing technique within the music industry. ICE's current seize-now-

[11] *See* Ben Sisario, "Piracy Fight Shuts Down Music Blogs," *N.Y. Times* (Dec. 13, 2010), *available at* <http://www.nytimes.com/2010/12/14/business/media/14music.html?_r=1&ref=todayspaper>.

[12] Ben Sisario, "Piracy Fight Shuts Down Music Blogs," *supra* n. 11.

[13] Letter from Senator Ron Wyden to The Honorable John Morton, Director, U.S. Immigration and Customs Enforcement 2, *supra* n. 10.

and-worry-about-it-later approach opts to hit operators with the excessively harsh sanction of not only seizing the domain, but also stigmatizing the operator with ICE's placeholder screen notifying visitors of the seizure, all without confirming whether or not the content has been posted with consent. COICA's approval of such a procedure will only serve to chill speech and completely shut down an innovative and useful marketing tool, as operators will likely cease posting material, even if they have been given permission to do so, for fear of the potential ICE repercussions.

**III. Domain Name Seizure as Proposed by S.3804 (COICA) Will Be Ineffective and Risky.**

COICA aims to address foreign websites that are otherwise beyond the reach of the U.S. legal process and are exclusively dedicated to making infringing content available to users in the U.S. and elsewhere. Unfortunately, COICA's scope goes far beyond its stated intent, and its remedies are not even likely to be effective.

A. COICA's Domain Name Blocking Will Be Ineffective.

Like the current domain name seizure exercises, COICA will have little practical impact on reducing infringement. COICA's primary strategy is to require that certain Internet intermediaries "de-list" sites from the Domain Name Server ("DNS") system – the virtual Internet "White Pages" that connect web servers' easy-to-remember domain names (like cnn.com) to their unique IP address number (157.166.226.25). Yet users can simply point their browsers to IP addresses instead of domain names, or easily configure their computers to use one of millions of offshore 'phone books' (DNS servers), thereby circumventing the restriction. Moreover, COICA's domain name provisions will have limited effect on non-U.S. Internet users, since their DNS servers cannot be compelled to purge domain name entries by U.S. authorities.

A COICA-based seizure of 'cnn.com' means that 'cnn.com' will no longer direct to the IP address 157.166.255.19. The website will not disappear. Instead of typing 'cnn.com' into their browser bar, users will simply enter the 11-digit string that is the IP address, and access CNN. A domain name seizure or a domain name block is like tearing a page out of a phonebook to prevent people from dialing the "bad" number. The relevant page may be missing from the phonebook – the DNS server – but the "bad" phone line – the IP address – hasn't been disconnected. Everyone who knows the number may still dial it. Moreover, users can circumvent the blocking by employing another phonebook (DNS server) through a simple

change of their browser settings. Even *supporters* of COICA have conceded that changing DNS servers is "incredibly easy".[14]

When Wikileaks' DNS server was under cyberattack in late 2010, the site's IP address was a top search result on all major search engines, and could also be easily discovered on numerous online forums or in news articles discussing the dispute. Users simply copied "*213.251.145.96*" into the address bar of their browser and easily accessed Wikileaks. Ultimately, the cyberattack on Wikileaks' server that caused the site's domain name to fail had little effect on the site's availability.

B. COICA Will Have Troublesome Collateral Consequences.

The scope and application of COICA (i) is significantly broader than its stated intent; (ii) is inconsistent with existing law; (iii) deputizes the private sector into law enforcement without compensation; and (iv) sets bad precedents. COICA unnecessarily applies to domestic sites, and the breadth of its definitions improperly sweeps in online retailers, web platforms and cloud storage services, as well as entirely legal products and services sold on lawful websites. Moreover, it endangers cybersecurity and sets bad precedents for broader blocking by foreign governments.

*COICA Inappropriately Extends to Domestic Sites.* Although it purports to address the "worst of the worst" foreign pirates, COICA in fact applies to U.S. domestic websites, permitting U.S. law enforcement to forego standard due process procedures that should be afforded to Americans. This is unnecessary, given the current strong IP enforcement in the United States.

As the committee is aware, it remains unclear how COICA would interact with the Digital Millennium Copyright Act (DMCA).[15] Insofar as COICA is an extraordinary remedy, to be used only in cases where a foreign website cannot be reached through regular U.S. legal channels, COICA currently does not address its potential to supersede the DMCA's provisions that allow website operators the opportunity to appear in court and defend themselves against allegations of hosting infringing content.[16] COICA thus appears to be both duplicative and inconsistent with existing protections.

[14] Daniel Castro, "No, COICA Will Not Break the Internet," Innovation Policy Blog, The Information Technology and Information Foundation (Jan. 18, 2011), *available at* <http://www.innovationpolicy.org/no-coica-will-not-break-the-internet>.

[15] *See* Letter from Markham C. Erickson, Executive Director, NetCoalition, to The Honorable Patrick Leahy, Chairman, Senate Committee on the Judiciary, *supra* n. 5.

[16] *Id.* at 1-2 (discussing 17 U.S.C. § 512(g)(3)).

*COICA's Overbroad Definition Sweeps in Legitimate Online Sites and Legal Products and Services.* COICA defines as infringing all websites that offer goods or services that enable a violation of copyright law. As years of litigation have shown, iPods, VCRs, personal computers, photocopiers, and countless consumer electronics all *enable* violations of copyright law. Yet under COICA's definitions, legitimate sites selling these electronic products are "dedicated to infringing activities."

Due to the many uses of "or" in COICA's definition of what sites are "dedicated to infringing activities", COICA sweeps in many legitimate domains. Any domain name may be seized so long as the site "is marketed by… a person acting in concert with the operator… to offer goods or services… that enable… a violation of title 17… when… such activities are the central activities of the Internet site." COICA § 2(a)(1)(B)(i)(I-II). Under COICA's definition, Best Buy's website may be "dedicated to infringing activities." If Best Buy advertises that one may buy iPods and PCs on bestbuy.com, the domain could be subject to a COICA seizure, since iPods and PCs "enable" "violation[s]" of title 17 and selling iPods and PCs is central to bestbuy.com's activities. Unless COICA aims to punish all consumer electronics vendors, this provision in particular demands revision.

In addition, because COICA lacks any willfulness requirement, any service used in infringement totaling more than $1,000 may be targeted. This affects numerous legitimate online services, and appears even to include the U.S. Postal Service, given the recent indictment of a Baltimore man who received over $265,000 for infringing software he distributed online and via U.S. Mail.[17] Neither the online services nor the Post Office are guilty parties in this offense.

*COICA endangers cybersecurity.* Dan Kaminsky, the famous security researcher credited with "saving the Internet" has said COICA is dangerous.[18] Kaminsky, who discovered a critical security bug in the architecture of the domain name system (which now bears his name), has noted that one of COICA's risks arises from the fact that patching the "Kaminsky bug" requires users to trust DNS servers. COICA undermines that trust by demanding that DNS servers occasionally deny users' requests – effectively lying about where sites are. COICA could thus

[17] *See* "Maryland Man Indicted for Infringement of Commercial Software Programs," ICE News Release (Jan. 14, 2011), *available at* < http://www.ice.gov/news/releases/1101/110114baltimore2.htm>.

[18] Jack Schofield, "How Dan Kaminsky Saved the Internet", The Guardian (Dec. 2, 2008) *available at* <http://www.guardian.co.uk/technology/blog/2008/dec/02/dns-kaminsky>; *see also* Dan Kaminsky, *DNS Filtering and S.3804, 'Countering Online Infringement and Counterfeiting Act'*, *supra* n.1.

impede efforts to patch this security flaw by driving users to unsecure, offshore servers.[19] First, COICA's requirement to block certain domain names will encourage users to switch from the name servers provided by their ISPs over to offshore servers, thus hindering the U.S. government's ability to respond to cyber attacks. Such a shift could also hinder network managers' ability to monitor activity over their networks and the ability to get any necessary software patches out to users. The ease with which users can adopt offshore name servers which will not be bound by COICA's requirements would therefore undermine COICA's impact while increasing the exposure of the U.S. infrastructure to cyberattack.[20]

By requiring *ad hoc*, manual editing of DNS databases, COICA may also impede the implementation of DNS Security Extensions (DNSSEC), a ten-year project to increase Internet DNS security.[21] DNSSEC figures prominently in the White House's strategy for increasing security on the .gov, .edu, and .us top level domains (TLDs).[22]

Moreover, the Pirate Bay has recently announced that it will start providing its own uncensored DNS server. Users will be told that if they use Pirate Bay's 'phonebook,' they will have a censorship-free experience. Such a DNS server may become an attractive nuisance target for cyberattacks designed at exploiting its control over traffic, and it is uncertain whether Pirate Bay or any other ideologically motivated provider of a DNS server will have the requisite security. The operator of an unofficial, unsecure DNS server might decide to redirect Internet traffic for a political purpose. The result is that its DNS server might one day direct users of 'bankofamerica.com' or 'whitehouse.gov' to a malicious site, rather than their intended destination.

*COICA sets bad precedents that will be used to justify foreign blocking of U.S. services.* COICA's expansive interpretation of the jurisdiction of the Federal Government, and its effectively extraterritorial application of U.S. law, all come at a time when authoritarian governments are seeking greater control over Internet architecture, and foreign officials are demanding that the ITU, a UN agency, take control of Internet governance functions from the

[19] *See* Letter from Markham C. Erickson, Executive Director, NetCoalition, to The Honorable Patrick Leahy, Chairman, Senate Committee on the Judiciary 3, *supra* n.5.
[20] *Id.*
[21] *See* Kaminsky, *supra.*
[22] White House Strategy for American Innovation: Securing Our Economic Growth and Prosperity (Feb. 2011) Appx. A *available at* <http://www.whitehouse.gov/innovation/strategy/appendix-a>.

U.S.-based independent non-profit ICANN.[23] Furthermore, the precedent of COICA may invite retaliation against U.S. businesses and will disadvantage U.S. efforts to maintain a free and open Internet. Similar concerns have motivated human rights advocates who fear that the U.S. is setting a precedent of filtering and blocking websites based on content that will abandon the moral high ground in the Administration's efforts to secure the ability for Internet users across the globe to access the legal content of their choice[24] - efforts which were reaffirmed just yesterday by Secretary Clinton in her speech on Internet Freedom at George Washington University. Human rights advocates also argue that COICA could lead to other countries using similar policies to prohibit access to legal U.S. content or, even worse, be used for political repression.[25]

C. COICA lacks proper safeguards.

Traditionally, law enforcement assistance bills contain proper safeguards to guard against abuse. COICA lacks such safeguards, including compensation to intermediaries when they are forced to provide services to the Federal Government, and restrictions on misuse.

*COICA's Mandate for the Private Sector is a Government Taking*. Unlike most other law enforcement assistance measures, COICA forces communications intermediaries to provide law enforcement assistance to the government free of charge. Whereas CALEA, ECPA, and the USAPATRIOT Act amendments all reimburse intermediaries when they are compelled to provide government services, COICA requires private entities to provide free, expeditious service to the Federal Government without any reimbursement or compensation.

*COICA includes a "vigilante" provision* that immunizes registrars and registries, financial transaction providers, and advertising services who voluntarily take Internet restricting actions against an Internet site if they "reasonably believes the Internet site is dedicated to infringing activities." Sites erroneously targeted are entitled to no protection and, if a site is intentionally targeted by a competitor, the vigilante provision appears to immunize that

[23] Omar El Akkad, "The Internet Needs Peacekeepers. Is Canada Ready?," *The Globe and Mail* (Nov. 12, 2010), *available at* <http://www.theglobeandmail.com/news/national/time-to-lead/internet/the-internet-needs-peacekeepers-is-canada-ready/article1795954/>.

[24] *See* Letter from American Civil Liberties Union, Center for Democracy & Technology, Electronic Frontier Foundation, Freedom House, Human Rights First, Human Rights Watch, Rebecca MacKinnon, Reporters Sans Frontières, and World Press Freedom Committee to Chairman Patrick J. Leahy and Ranking Member Jeff Sessions 1, *supra* n.2.

[25] *Id.* at 1-2.

competitor from any penalty, so long as this blocking is justified with the fig leaf that the site was believed to be "dedicated to infringing activities."

## IV. Alternatives to COICA

Fruitless tinkering with Internet architecture will not substitute for demands upon nations in the international trade community that they uphold the existing international IP laws they have committed to as a condition of participating in the global marketplace via the World Trade Organization. The U.S. can address true pirate sites operating abroad by insisting that foreign countries uphold their international commitments and enforce copyright law against the offenders. The U.S. has signed numerous Free Trade Agreements, and is one of over 150 nations that have joined the TRIPS Agreement, both of which require signatories to adhere to 'gold-standard' international IP norms. The USTR can bring countries who refuse to enforce their IP law before the WTO and demand that they be punished, as it has successfully done with China.[26] If the U.S. is unwilling to enforce trading partners' commitments to protect IP, then it will have squandered precious political capital in securing these agreements in the first place. The benefits of an international approach – in addition to avoiding the Internet-crippling security risks posed by COICA – are that when sites are taken down, they disappear worldwide. COICA, on the other hand, would merely inconvenience U.S. Internet users, imposing minor, transitory hurdles that COICA supporters concede are easily defeated.

## V. Conclusion

In conclusion, I urge the committee to avoid putting an American seal of approval upon a strategy most frequently employed by strongmen and despots. The threat to Internet freedom posed by government control over the private sector-maintained Internet architecture is immense. Perhaps even more importantly, as we have already seen, it would not address the stated problem. The approach to insufficient law enforcement must be more law enforcement, not government authority over Internet domains.

[26] Panel Report, *China – Measures Affecting the Protection and Enforcement of Intellectual Property Rights*, WT/DS362/R (Jan 26, 2009), *available at* <http://www.wto.org/english/tratop_e/dispu_e/cases_e/ds362_e.htm>.