Written Testimony Submitted for the Record of

Daniel Castro

Senior Analyst, Information Technology and Innovation Foundation (ITIF)

on

"Targeting Websites Dedicated To Stealing American Intellectual Property"

before the

Senate Committee on the Judiciary

U.S. Senate

February 12, 2011

Legislation introduced in Congress in 2010, such as S. 3804, the "Combating Online Infringement and Counterfeits Act" (COICA), would take an aggressive and needed stand against online piracy and counterfeit goods, a growing problem that hurts American consumers and costs Americans jobs. Critics of the legislation argue that this bill would hurt free speech, encourage censorship in foreign countries, and cripple the technological infrastructure on which the Internet runs. Not only is this criticism untrue, but more robust enforcement of digital copyrights would likely lead to a stronger Internet ecosystem and more innovative content and services for consumers.

The Problem of Digital Piracy

Software, video games, movies, music, books, photos, and other media are increasingly available to users online. Many users go online and pay for digital content or applications through sites like Amazon, iTunes or Netflix. And the advent of new services like Google TV suggests that consumers will increasingly use the Internet to enjoy video programming on their PCs, in their living rooms and on their mobile devices. But all too many Internet users are choosing to download pirated digital content from illegal sites or peer-to-peer (P2P) networks. The problem has become some pervasive that at least 1 in 4 bits of traffic on the Internet is related to infringing content.[1] The Information Technology and Innovation Foundation (ITIF) has previously documented how Internet users can easily go online and, with just a few clicks, find pirated copies of full-length Hollywood movies or television programming to watch for free or software programs to use on their computers.[2] Many of these sites earn advertising dollars from major companies. For example, in ITIF's 2009 review of the websites The Pirate Bay and isoHunt, we found brands such as Amazon.com, Blockbuster, British Airways, and Sprint appearing on these sites.[3]

Online piracy has a significant impact on the U.S. economy. While the exact cost of piracy is difficult to measure, the impact is substantial, with one estimate finding that the U.S. motion picture, sound

recording, business software, and entertainment software/video game industries lost over $20 billion dollars in 2005 due to piracy, and retailers lost another $2 billion, for a combined loss of over $22 billion.[4] Online piracy harms the artists, both the famous and struggling, who create content, as well as the technicians—sound engineers, editors, set designers, software and game programmers—who produce it. Piracy ultimately also hurts law-abiding consumers who must pay higher prices for content, enjoy less content or relatively lower quality content, or pay higher prices for Internet access to compensate for the costs of piracy.

Potential Legislative Responses

In December 2009, ITIF proposed a number of policies to help reduce online copyright infringement, especially in countries that turn a blind eye to copyright enforcement.[5] These recommendations include the following:

- Create a process by which the federal government, with the help of third parties, can identify websites around the world that are systemically engaged in piracy
- Enlist ISPs to combat piracy by blocking websites that offer pirated content
- Enlist search engines to combat piracy by removing websites that offer infringing content from their search results
- Require ad networks and financial service providers to stop doing business with websites providing access to pirated content
- Create a process so that the private sector can consult with government regulators on proposed uses of anti-piracy technology
- Fund anti-piracy technology research, such as content identification technology
- Pursue international frameworks to protect intellectual property and impose significant pressure and penalties on countries that flout copyright law

Many of these recommendations have been considered in recent legislation, such as COICA, introduced by Senators Patrick Leahy (D-VT) and Orrin Hatch (R-UT) in 2010. COICA would provide important new tools to crack down on online infringement of intellectual property. The legislation would not target minor violations of copyright, but rather would target "Internet sites dedicated to infringing activities" which it defines as a site that is "primarily designed, has no demonstrable, commercially significant purpose or use other than, or is marketed by its operator…to offer" unauthorized access to copyright-protected content.

Response to Criticism of Legislation

Critics of COICA make three general objections: 1) that the legislation would impair free speech; 2) that the legislation would encourage censorship in foreign countries; and 3) that the legislation would cripple the technological infrastructure on which the Internet runs. All of these objections are unfounded.

Freedom of Speech

First, some critics oppose the legislation on the grounds that it would hurt free speech, a groundless accusation. Not all free speech is protected. As Justice Holmes in *Schenck v. U.S.* famously argued, freedom of speech does not include the freedom to falsely yell "Fire" in a crowded theater (or more recently "Bomb!" on an airplane).[6] Nor does it entail a freedom to establish a website for the sole purpose of enabling online piracy, even if the site posts a few statements expressing the owners' political views.

Neither does the idea of a "free and open" Internet mean that every website has the right to exist. Certainly, most people would agree that some websites should not be permitted to remain online, such as sites devoted to hosting child pornography or illegal scams. The purpose of this legislation is not to shut down a personal website that accidentally links to a copyrighted image or websites that use material protected by fair use, but to shut down websites whose principal purpose is to engage in egregious infringement of intellectual property.

Yet critics of the legislation, such as the Electronic Frontier Foundation (EFF), complain that free speech will be hurt if the government blocks "a whole domain, and not just the infringing part of the site."[7] While certainly most infringing sites will contain at least some non-infringing content, it is not an injustice to block the entire site. As noted, the legislation only applies to sites where the principal purpose of the site is to engage in digital piracy. Such frivolous complaints are equivalent to arguing that the justice system would be unfair to shut down a bar found to be repeatedly serving alcohol to minors even if some of its customers were of legal age or a pawn shop that serves as a front for moving stolen goods even if a few of its items were acquired legally.

Others present a similar criticism of the legislation under the guise of protecting free speech when their objection is really to an expansion of government authority. This mentality is exemplified by Bruce Schneier who as a matter of course argues against virtually any action by government to police abuses on the Internet.[8] These kinds of objections come from a purely anti-government ideology that rejects any attempt to give government more power, even if that is appropriate power to enforce laws against criminals.

Foreign Censorship

Critics also claim that COICA would set a negative precedent and harm the United States internationally by giving political cover to the "totalitarian, profoundly anti-democratic regimes that keep their citizens from seeing the whole Internet."[9] Critics, such as the 87 Internet engineers who signed EFF's letter to the Judiciary Committee, argue that the legislation would "seriously harm the credibility of the United States in its role as a steward of key Internet infrastructure." Others, including groups like the American Library Association, Consumer Electronics Association, NetCoalition and Public Knowledge, argue that "COICA's blacklist may be used to justify foreign blacklists of websites that criticize governments or royalty, or that contain other 'unlawful' or 'subversive' speech."[10] Again, these criticisms do not stand up to a serious analysis. This is equivalent to arguing that the United States should not put rioters who engage in wholesale property destruction and violence in jail because it simply encourages totalitarian governments to use their police to suppress their citizens.

More narrowly, some critics, such as Wendy Seltzer at Princeton University's Center for Information Technology Policy, argue that other countries would use anti-piracy efforts as a ruse for cracking down on political dissidents.[11] Such activities are not without precedent—Russian police have raided advocacy groups and opposition newspapers that have spoken out against the government in the name of searching for pirated software.[12] Yet while certainly some unscrupulous countries might claim their actions are equivalent to that of the United States, it would be demonstrably untrue. There is simply no comparison between a country using clear and transparent legal means to enforce intellectual property rights online and a country censoring political speech online, even under the guise of protecting copyrights. Moreover, to argue that abusive regimes operating without the rule of law would somehow act more abusively because the United States cracks down on cyber crime is a stretch at best. If this were the case, we should have seen a dramatic increase in Internet censorship after nations like France and the U.K recently passed laws to crack down on online copyright theft.

In fact, if this law would have any effect on foreign nations it would be to embolden them to take stronger steps to crack down on digital piracy, a problem that is even worse in many foreign nations and one that contributes to a deteriorating balance of trade for the United States as foreign consumers steal U.S. software, music, video games, movies, books, photos, and other digital content.

Weaken the Internet

Finally, some opponents of stricter online IP enforcement argue that this legislation "will risk fragmenting the Internet's global domain name system (DNS)."[13] To understand the debate, you must understand how DNS works. DNS is like a global phonebook for the Internet providing users a number that corresponds to each name. Before a user can visit a domain name (e.g. www.itif.org), his or her computer must first discover the IP address associated with that web address (e.g. 69.65.119.60). DNS servers provide this service to users by translating domain names into IP addresses through a recursive process. Most users rely on the DNS servers of their local ISP for this service and it is these DNS servers that are the principle target of COICA. If a site appeared on the government blacklist, e.g. www.watch-pirated-videos.tv, then the DNS servers would be instructed to no longer resolve an IP address for that domain. And without this IP address, users cannot visit these infringing websites.

Groups like EFF claim this will "undermine basic Internet infrastructure" and lament that it will keep ISPs from "telling you the truth about a website's location."[14] While such fiction may be useful in generating fear about COICA, the simple fact is that using DNS to block access to websites or servers is not new or particularly challenging—it has been used for blocking spam and protecting users from malware, for example, for many years. In addition, many DNS resolvers routinely return different answers to users as part of a service, such as to provide parental filters, correct typos in URLs, or to provide search results in lieu of a basic "domain not found" error.[15]

Other critics, such as the Center for Democracy and Technology, argue that COICA will set a precedent where ISPs will be required to block other "illegal or unsavory content" creating "a controlled, ISP-policed medium."[16] Such an end result is antithetical to the worldview of CDT (and other opponents of this legislation) that the Internet should be free of private-sector control regardless of the consequences. This "slippery slope" argument is fundamentally illogical. The analogy would be like

saying that if we pass laws against a person committing physical assault on another person, then it is only a matter of time before we pass laws against people bumping into each other rudely on the street. Such stubborn and entrenched views do not reflect the kind of flexible policymaking that most people agree is necessary for the fast-paced world of the evolving Internet. Rather than relying on tradition to justify Internet policy, a better approach would be to look at the practical implications of specific policy proposals in the present.

Why the Criticism?

So what's really behind these criticisms? They all reflect these groups' and individuals' overarching view of the Internet as a medium whose chief function is to liberate individuals from control by, or dependence on, big organizations. For these groups, the Internet is first and foremost about individual freedom, not about collective responsibility. They see the Internet as a special place, above and beyond the reach of the kinds of rules that govern the offline world. Yet, for most of the rest of us, the Internet is no different than the rest of society where we have rights and responsibilities and where laws against certain behaviors exist. We play by the rules and we expect others to do the same, and when they do not, we expect society (through the actions of democratically elected governments) to step in and punish those who commit crimes. All of these objections listed here reflect this fundamental Internet exceptionalist ideology, and as such are largely attacks not so much on this particular legislation, but on any legislation that would put limits on Internet freedom, even if it's the freedom to falsely yell "fire!" in a crowded theatre.

Because of their overriding focus on individual freedom and not on collective benefit, critics of the legislation fail to understand that stronger enforcement of intellectual property would be beneficial to American consumers and businesses. For example, delivering video content to the TV is expected to be the next driver of broadband access and services but for this business model to work, content owners and creators should be able to ensure their rights are protected. Online piracy not only results in the unauthorized distribution of content, it hurts the ability of content producers to create legitimate business models for selling digital content. As the saying goes, "It's hard to compete with free." While many companies have rallied to the challenge and created compelling businesses to sell content legally, on the whole, illegal content still remains widely available and commonplace.

Conclusion

COICA is important because it recognizes that online piracy is no longer about college students trading files in their dorm room, but instead it has grown in to a multi-million dollar international business. Sites hosting pirated content or linking to pirated content can generate a significant amount of revenue from online advertising and sales. COICA would provide a mechanism to not only cut off access to these sites, but also cut off their funding mechanisms to make operating online piracy sites unprofitable.

Should we throw out freedom of speech and long-held legal protections like due process just to protect intellectual property online? Of course not. But neither should we abandon the Constitutional provisions which support protecting intellectual property. As with any law enforcement initiative, efforts at

reducing online piracy involve balancing costs and benefits. While street crime could be reduced by doubling the number of police, most communities find an equilibrium where the marginal cost of an additional police officer does not outweigh the corresponding reduction in crime. With regard to Internet piracy, it is hard to argue that this equilibrium has been reached and that society would not be better off with greater efforts to stop digital piracy. While not all anti-piracy efforts should be embraced—for example, policymakers are wise to shy away from expensive digital rights management (DRM) technology mandates—the government should make a serious effort to combat piracy through reasonable approaches like COICA. The extent of piracy is so large, and the costs of enforcement quite reasonable, that it is clearly in the public interest to take more aggressive steps to curb it. Legislation such as COICA provides an opportunity for the U.S. government to get serious about enforcing intellectual property rights online.

---

[1] David Price, "An Estimate of Infringing Use of the Internet," Envisional (2011), http://documents.envisional.com/docs/Envisional-Internet_Usage-Jan2011.pdf.

[2] Daniel Castro, Richard Bennett, and Scott Andes, "Steal These Policies: Strategies for Reducing Digital Piracy," Information Technology and Innovation Foundation (Washington, DC: 2009), http://www.itif.org/files/2009-digital-piracy.pdf.

[3] Ibid.

[4] Stephen Siwek, "The True Cost of Copyright Industry Piracy to the U.S. Economy," Policy Report 189, The Institute for Policy Innovation, September 2007.

[5] Castro, Bennett and Andes, "Steal these Policies."

[6] "The man who said 'bomb' on an airplane," San Francisco Chronicle, August 6, 2010, http://www.sfgate.com/cgi-bin/blogs/crime/detail?entry_id=69558 and "Woman accused of airport bomb threats," United Press International, April 21, 2008, http://www.upi.com/Top_News/2008/04/21/Woman-accused-of-airport-bomb-threats/UPI-38521208794796/.

[7] Richard Esguerra, "Censorship of the Internet Takes Center Stage in 'Online Infringement' Bill," Electronic Frontier Foundation, September 21, 2010, http://www.eff.org/deeplinks/2010/09/censorship-internet-takes-center-stage-online.

[8] For example, with regards to the Obama Administration's plans to expand wiretapping online Schneier writes, "it's bad civic hygiene to build technologies that could someday be used to facilitate a police state." Bruce Schneier, "Web snooping is a dangerous move," CNN.com, September 29, 2010, http://www.cnn.com/2010/OPINION/09/29/schneier.web.surveillance/index.html.

[9] Esguerra, "Censorship of the Internet Takes Center Stage in 'Online Infringement' Bill."

[10] Letter from Public Knowledge et al. on "S. 3804, Combating Online Infringement and Counterfeits Act (COICA), September 27, 2010, http://www.publicknowledge.org/files/docs/JointLetterCOICA20100929.pdf.

[11] Wendy Seltzer, "Copyright, Censorship, and Domain Name Blacklists at Home in the U.S.," Freedom to Tinker, September 21, 2010, http://www.freedom-to-tinker.com/blog/wseltzer/copyright-censorship-and-domain-name-blacklists-home-us.

[12] Clifford Levy, "Russia Uses Microsoft to Suppress Dissent," New York Times, September 11, 2010, http://www.nytimes.com/2010/09/12/world/europe/12raids.html.

[13] Peter Eckersley, "An Open Letter From Internet Engineers to the Senate Judiciary Committee," Electronic Frontier Foundation, September 29, 2010, http://www.eff.org/deeplinks/2010/09/open-letter.

[14] Esguerra, "Censorship of the Internet Takes Center Stage in 'Online Infringement' Bill."

[15] For a more detailed rebuttal of some of the technical fears about COICA, see Daniel Castro, "No, COICA Will Not Break the Internet," Innovation Policy Blog (2011), http://www.innovationpolicy.org/no-coica-will-not-break-the-internet.

[16] "The Dangers of S. 3804: Domain Name Seizures and Blocking Pose Threats to Free Expression, Global Internet Freedom, and the Internet's Open Architecture," Center for Democracy and Technology, September 28, 2010, http://cdt.org/files/pdfs/Leahy_bill_memo.pdf.