

Daniel Castro  
Senior Analyst  
Information Technology and Innovation Foundation (ITIF)

“Promoting Investment and Protect Commerce Online: Legitimate Sites vs. Parasites, Part I”

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

March 14, 2011

Mr. Chairman and members of the Committee, I appreciate the opportunity to appear before you to discuss how to promote investment and protect commerce online by creating new enforcement mechanisms to restrict the impact of parasitic websites. These websites are an economic leech on the Internet economy. My name is Daniel Castro. I am a senior analyst at the Information Technology and Innovation Foundation (ITIF). ITIF is a nonpartisan research and educational institute whose mission is to formulate and promote public policies to advance technological innovation and productivity.

The Internet is a tremendous enterprise of user empowerment, free speech, and innovation, but it facilitates unlawful acts just as much as lawful ones. The proliferation of parasitic or rogue sites—websites enabling online piracy and the trade of counterfeit goods at the expense of legitimate businesses—is a pervasive problem that hurts American consumers and costs Americans jobs. Unchecked these rogue sites are a threat to the economic welfare of the United States.

While there is no silver bullet for stopping these rogue sites, we have an arsenal of “lead bullets” that collectively can significantly reduce their impact and sustainability. As with any law enforcement initiative, efforts at reducing digital piracy and online counterfeiting involve balancing costs and benefits. For example, while street crime could be reduced by doubling the number of police officers, communities seek an equilibrium where the marginal cost of an additional police officer does not outweigh the corresponding reduction in crime. With regard to rogue sites, it is hard to argue that this equilibrium has been reached—that society would not be better off with greater efforts to stop these sites. The extent of online copyright infringement is so large, and the costs of additional enforcement are so reasonable, that it is clearly in the public interest to take more aggressive steps to curb it.

Critics of stronger online intellectual property (IP) enforcement claim that such efforts will negatively impact the Internet ecosystem. This claim seems to assume that piracy is the bedrock of the Internet economy, an assertion not backed up by any evidence. Rather than limiting Internet innovation, as some assert, protecting copyrighted works online is necessary for innovation to continue to thrive on the Internet. While some anti-piracy proposals impose too much of a burden on businesses and consumers, many anti-piracy efforts do not negatively impact the Internet ecosystem. The goal of policymakers should be to identify and encourage as many of these tools and techniques as possible.

While the Internet is a vast, distributed system that has no central point of control, it should not be without any control whatsoever. Rather, the responsibility for maintaining the Internet falls upon each user, each service provider, and each business and institution that uses it, operates it, and benefits from it. Not every effort targeted at rogue sites should be embraced. But there are many cost-effective technologies available to confront rogue sites that only impinge on the “freedom” to steal. The U.S. government needs to put in place a framework that facilitates and encourages responsible control by all. Much more can and should be done. We need to make sure that all stakeholders, including government, content owners, website operators, financial service providers, ad networks, search engines, ISPs and other intermediaries, work together to form a comprehensive response to rogue sites.

## **Rogues Sites Remain a Significant Problem for the United States**

Rogue sites—websites engaged in digital piracy or selling counterfeit goods—steal U.S. intellectual property and stunt economic growth, eliminate American jobs, and put U.S. consumers at risk. As documented here and elsewhere, intellectual property (IP) makes substantial contributions to the U.S. economy. IP enforcement is an increasingly urgent matter for the United States because IP is a large component of what the United States produces and because this content is increasingly vulnerable in the global, knowledge-based economy. While U.S. firms increasingly manufacture overseas, an estimated 45 percent of the U.S. GDP comes from the proprietary ideas inside a product rather than the assembly of products.<sup>1</sup> The United States is a net exporter of IP, with IP contributing \$37 billion to our trade balance in 2006.<sup>2</sup> IP industries also contribute to the U.S. trade balance through royalties and licensing fees. In 2006, U.S. receipts from cross-border trade in royalties and license fees (including patents, trademark, copyright, and other intangible rights) amounted to \$63.4 billion and payments totaled \$26.4 billion.<sup>3</sup>

The costs imposed on businesses by digital copyright infringement and counterfeiting restrict the ability of innovators to recover the expenses they incur to develop new products and services or produce new content. These activities reduce investment in research and development for new technology, lower U.S. economic growth, and ultimately result in a less robust innovation economy.

## Online Piracy

Of all the industries that have been revolutionized by the rise of digital technology and the global Internet, few have been hit as hard as the industries that produce creative works—the producers of software, music, movies, television programs, video games, books, photos, and other media. The Internet has made global distribution of content easier than ever, with the ultimate promise of slashing costs by reducing the role of middlemen who produce, distribute, and sell the physical copies. Many users go online and pay for digital content or applications through sites like Amazon, iTunes or Netflix. Unfortunately, the digital era also has a serious downside for content producers and others in the industry as it has made it easier than ever for consumers to get access to content without authorization or without paying for it. Many Internet users around the world still choose to download pirated digital content from illegal sites or peer-to-peer (P2P) networks. The problem has become so pervasive that one in four bits of traffic traveling on the Internet today is infringing content.<sup>4</sup>

Much of the illegal exchange of content has been facilitated by digital tools that facilitate file sharing between users, including peer-to-peer (P2P) file sharing networks, hosted online file shares and online streaming services. P2P-based and unicast streaming services such as TVAnts and SopCast are widely used for re-transmission of live sports games and other events.<sup>5</sup> While all of these technologies have legitimate uses, the technologies have also been used for the unauthorized distribution of digital content on a global scale. In some cases, such as with some P2P file sharing networks, this has even become the principal use of the technology, although some P2P networks are focused on distributing legal content.<sup>6</sup> Websites like the Pirate Bay, isoHunt, and Btjunkie routinely rank among the most popular websites on the Internet and offer the ability to illegally download virtually all popular TV series, movies, recently released songs, software and games.<sup>7</sup> Unauthorized file sharing has been exacerbated by the growth of Web 2.0, or websites that cater to user-generated content, as many Internet users make no distinction when uploading between content they are authorized to upload and content they are not.

ITIF has previously documented how Internet users can easily go online and, with just a few clicks, download pirated copies of full-length Hollywood movies, watch unauthorized live video streams of sports programming online for free, or illegally download software programs to use on their computers.<sup>8</sup> To give just one example, a recent web search for “Watch Inception Online” did not yield a single link to a legitimate website in the first two pages of results, but instead produced links to rogue sites to watch or download the movie.<sup>9</sup> Many of these sites earn advertising dollars from major companies. In ITIF’s 2009 review of the websites The Pirate Bay and isoHunt, we found these sites displaying ads for brands such as Amazon.com, Blockbuster, British Airways, and Sprint.<sup>10</sup>

Some argue that online piracy is not really a problem, and that it only hurts large, profitable multinational companies, and even helps consumers by enabling them to obtain content at no cost. But this is fundamentally wrong. 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. And it 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. Moreover, digital 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.

While most individuals do not shoplift DVDs out of retail stores, many people feel comfortable downloading movies without paying for them. Why do so many people knowingly choose to continue to download unauthorized content? One reason is that it is so easy to find and download copyrighted content online. If stealing cars was as easy as pointing and clicking (and no one could tell if the car you are driving is stolen), the rate of motor vehicle theft would probably be much higher. A Pew Report found that “75% of teen music downloaders ages 12-17 agree that ‘file-sharing is so easy to do, it’s unrealistic to expect people not to do it.’”<sup>11</sup> This survey also reflects the mentality of many people who think that “everybody is doing it” or that piracy is just “a function of the Internet.”<sup>12</sup> Moreover, the Internet gives users a sense of anonymity where the risk of getting caught is relatively low and that of punishment even lower.

Piracy has a negative effect on the U.S. economy. Because the United States is the nation that is most specialized in the production of digital goods (e.g., music, movies, software, video games, books, etc.) it also the nation that is most vulnerable to digital piracy. And much of this piracy occurs online. While the exact cost of piracy is difficult to measure, we have some good estimates of its magnitude. For example, one estimate found 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.<sup>13</sup> In 2006, another study found that the U.S. recording industry and related industries lost over \$3.5 billion to online piracy and approximately \$1.5 billion in physical piracy.<sup>14</sup> The recording industry has been particularly hurt by online theft because digital music files are small enough to transmit quickly, even over relatively slow Internet connections. The International Federation of the Phonographic Industry (IFPI) estimates that for every purchased track there are as many as 20 illegally downloaded songs.<sup>15</sup> In 2005, music piracy was associated with the loss or lack of realization of over 12,000 jobs in the sound recording industry in the United States.<sup>16</sup>

Other content industries have been impacted by piracy as well. The motion picture industry has lost significant amounts of money to pirated movies both online and on DVD. According to a report published by LEK Consulting, the U.S. motion picture industry lost \$6.1 billion to piracy in 2005, which one report argues eliminated or prevented the creation of 46,597 jobs in the motion picture industry.<sup>17</sup> Neither are software companies immune from piracy. With pirated

software equaling 20 percent of legitimate sales, the total value of pirated software is estimated to be over \$9 billion in the United States.<sup>18</sup> Moreover, although piracy rates have hovered around 20 percent for the last several years, total software piracy has steadily increased in line with the growth in software sales.

Online piracy of sporting events, either through distributing illegal recordings or retransmission of live events, is another pervasive problem. A 2008 study found that the audience for unauthorized live streams of sporting events, such as NBA, NFL and MLB games, exceeded one million viewers and users can often find numerous unauthorized live streams for popular events.<sup>19</sup> Sites streaming this content generate revenue either through ads or subscriptions. The impact of unauthorized transmissions is growing. For example, between 2007 and 2008 illegal distribution of Major League Baseball content increased by 25 percent.<sup>20</sup>

Videogame piracy is a growing problem worldwide. In 2008 the Entertainment Software Alliance detected more than 700,000 copyright infringements a month across more than 100 countries and sent out 6 million copyright infringement notifications. According to a report by the International Intellectual Property Alliance, in December 2008, 13 titles were illegally downloaded 6.4 million times. The top two titles alone accounted for nearly three-fourths of illegal downloads. The report, which evaluated piracy in 219 countries, found that two P2P networks, BitTorrent and eDonkey, were the largest sources of gaming piracy.<sup>21</sup>

Although not as common as music, movie, software, or videogame piracy, e-book piracy is growing, particularly as more content is sold in digital format. While hard data on book piracy is scarce, many publishing industry analysts see evidence of an alarming increase in piracy, due in part to the advent of the e-book reader. For example, John Wiley & Sons (publisher of the *Dummies* series) reports that in April 2009 it sent out 5,000 notices of online copyright violation—more than double the number of notices sent in the previous year.<sup>22</sup> In addition, e-book piracy appears to be more concentrated on certain websites than music, software, or motion picture piracy. Indeed, some industry observers estimated that as of 2009 as much as half of e-book piracy was housed on RapidShare, a Switzerland-based file hosting company that has advertised more than 10 petabytes of user uploaded files.<sup>23</sup>

## **Counterfeit Goods Online**

Rogue sites are also used to sell counterfeit goods. Counterfeit goods are widely available online through retail websites and online auctions. A recent study found that traffic to 48 sites selling counterfeit goods averaged more than 240,000 visits per day or more than 87 million visits per year.<sup>24</sup> Consumers shopping online are exposed to counterfeit goods, especially luxury goods such as jewelry, cosmetics, handbags, garments and shoes. Often these products are sold on sites that appear legitimate, charge reasonable prices, and may even link to the customer service of the brand owner. These counterfeit goods are often of poor quality. Counterfeiters also produce non-luxury goods. For example, counterfeit products such as infant formula or baby shampoo have also been discovered that pose health risks to young children. Illegal online pharmacies sell

counterfeit prescription and non-prescription drugs to consumers for a variety of health conditions. As best, these drugs may simply be ineffective; at worst, they can be harmful, even lethal, to human health. Statistics about the exact size of the global market for counterfeit drugs vary, but most experts agree the problem is serious.<sup>25</sup> A 2011 report found that the combined traffic to 26 sites selling counterfeit prescription drugs averaged 141,000 visits per day or more than 51 million visits per year.<sup>26</sup>

Counterfeiting hurts American consumers. First, consumers face financial losses. Consumers who unknowingly purchase counterfeit goods waste their money on inferior products. In addition, all consumers pay higher prices for goods as businesses must charge higher prices to recoup losses from the trade in counterfeit goods. Second, consumers risk physical harm. Counterfeit products can be unsafe, unmonitored for quality assurance, and pose a threat to human health. Injury and even death has been reported as a result of counterfeit baby formula, drugs, cosmetics and toiletries.<sup>27</sup>

Counterfeiting also hurts American companies. First, companies face direct losses from counterfeit goods that erode their sales. Second, consumers who unknowingly purchase low-quality counterfeit goods may mistakenly attribute the defects to the brand owner and no longer purchase products from that company. Companies must also allocate resources to responding to complaints from these “customers” who call to report defects or ask for service under an illegitimate warranty.<sup>28</sup>

Counterfeit goods account for approximately 7 percent of global trade.<sup>29</sup> The worldwide market for counterfeit goods exceeded \$500 billion in 2006 of which \$250 billion was for U.S. goods.<sup>30</sup> The impact of these losses is substantial. The International Anti-Counterfeiting Coalition estimates that counterfeit merchandise directly results in the loss of more than 750,000 American jobs.<sup>31</sup>

## **Potential Legislative Responses**

While the existing notice and takedown regime has provided an initial step towards combating piracy, clearly more can and needs to be done. Currently rogue sites operate in a low risk, high reward environment. Site operators, especially those outside of the United States, face few personal risks from law enforcement and encounter few barriers to distributing illegal content online. We need to change the equation. 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.<sup>32</sup> The purpose of these policies is to establish a robust enforcement mechanism to combat IP theft online. 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, allowing pricing structures and usage caps that discourage online piracy, and implementing notice and response systems
- Enlist search engines to combat piracy by removing websites that link to 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 the Combating Online Infringement and Counterfeits Act (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. Many of these “Internet sites dedicated to infringing” are well-known foreign websites in countries including Russia, Sweden and the Ukraine, such as the Pirate Bay and others identified in the USTR’s “Out-Of Cycle Review of Notorious Markets.”

## **Response to Criticism of Legislation**

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

### **Freedom of Speech**

First, some critics oppose COICA and similar proposals 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).<sup>33</sup> Nor does it entail the 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 or some other authorized content.

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.

There is no legitimate reason for parasitic websites, whose sole purpose is to leech off of the IP created by others, to exist. Russian piracy websites, like LegalSounds or other clones of the now defunct Russian website “allofmp3,” add nothing of value to the Internet economy and instead weaken it for all legitimate consumers and stakeholders. The Internet was not meant to be a gigantic piracy machine. It was not designed or built for the primary (or even secondary) purpose of facilitating unlawful transactions, and it is shameful for proponents of piracy to hide behind the excuse that filtering or blocking access to unlawful conduct is in some way analogous to the suppression of dissent in authoritarian dictatorships. There is clearly an enormous difference between the actions of an undemocratic government and the legitimate desire of liberal democracies to limit the ill-gotten gains of piracy promoters, advertisers, and service providers. The time has come for the law to catch up with technology by adopting a reasonable set of enforcement measures to make piracy less prevalent and less blatant on the Internet.

Yet critics of COICA, 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.”<sup>34</sup> 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, COICA 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 it would be unfair for the justice system 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 proposed legislative solutions 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.<sup>35</sup> 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 the policies in 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.”<sup>36</sup> Critics, such as the 87 Internet engineers who signed EFF’s letter to the Judiciary Committee, argue that COICA 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.”<sup>37</sup> 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 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.<sup>38</sup> 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.<sup>39</sup> 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).”<sup>40</sup> 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](http://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 the DNS server knows that a given domain name is for a rogue site, e.g. [www.watch-pirated-videos.tv](http://www.watch-pirated-videos.tv), then the DNS servers could be instructed to no longer resolve an IP address for that domain. And without this IP address, users would not be able to 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.”<sup>41</sup> While such fiction may be useful in generating fear about the policies in COICA, the simple fact is that using DNS to block access to websites or servers is not new or particularly challenging— DNS redirection has been used for blocking spam and botnets 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 control filters, correct typos in URLs, or to provide search results in lieu of a basic “domain not found” error.<sup>42</sup>

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.”<sup>43</sup> 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.

Finally, some critics lament that by preventing DNS servers from responding with “the truth, the whole truth, and nothing but the truth” COICA will sabotage DNS Security Extensions (DNSSEC), a recent upgrade to DNS that seeks to improve the security of the DNS system. Part of the problem is that the current DNS standard does not provide a mechanism by which a DNS server can tell the requester “the site may exist, but it is illegal so I am not going to find the answer for you.” Instead, the server must choose a less eloquent response, such as not replying (a bad idea since the user will just keep asking), replying that the domain does not exist, or replying with an incorrect address.

However, this problem appears to be the result of a deficiency in the current DNS protocol rather than any true technical limitation. It could be easily addressed by modifying the standard to support these additional types of responses. Indeed, one such modification has already been developed and proposed by a key architect of DNS.<sup>44</sup>

Other critics claim that DNS blocking will provoke a mass exodus of users from U.S.-based DNS servers to foreign DNS servers outside of the jurisdiction of U.S. lawmakers and, as a result, be ineffective. However, this argument is flawed. While switching DNS servers may be easy for some users, it is still beyond the comfort level of many, if not most, Internet users. Moreover, users who switch to foreign DNS servers would expose themselves to many security risks if they cannot trust the responses from these servers. For example, while the name servers may reliably return the correct IP address for a Russian MP3 site, they might not return the

correct address for Bank of America. How many users are willing to risk their identity and financial information just to download a few songs? Similarly, the DNS server that a person uses can collect a fairly detailed record of an individual's browsing history which presents obvious privacy risks. Would most users trust their entire browsing history to an unregulated, foreign company?

Using a foreign DNS server also could result in substantial decreases in performance for many users. People usually get what they pay for (except with piracy!), and a free foreign DNS service is likely to be substantially slower than the DNS servers offered by local ISPs. How many users would tolerate a few extra seconds of delay every time they click a link? In addition, users of foreign DNS servers would likely see another performance hit when accessing websites using content distribution networks like Akamai because foreign DNS servers would point them to the CDN content servers closest to the overseas DNS server not the user.

Aside from practical matters there is also the obvious question of who would be willing to provide such a service. If, as opponents of these policies argue, virtually every American user leaves their local DNS server, who would provide all of the computing power necessary to process these DNS requests? And more importantly, who would pay for it? Moreover, these opponents miss the point that these policies can be extremely effective even if some users evade the restrictions. Many users visit these sites out of ignorance or complacency. A warning that lets them know that the site they are trying to access is illegitimate will help direct consumers to legitimate websites for legal goods.

## **Why the Criticism?**

So what's really behind these criticisms? Most 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 COICA or similar proposals fail to understand that stronger enforcement of intellectual property would be beneficial to the American economy as it faces growing international competition. It is

one thing for U.S. companies and workers to compete against companies and workers in other nations that play by the rules. It is quite another thing to compete against other nations that systematically cheat and steal U.S. intellectual property.

## **Conclusion**

Stronger enforcement mechanisms are necessary. Online piracy is no longer a hobby among college students trading files in their dorm room, but instead it has grown in to a multi-million dollar international business that is leeching jobs and investment out of the American economy. Sites hosting pirated content or linking to pirated content can generate a significant amount of revenue from online advertising and sales and easily cover their expenses. The policies that we recommend would provide a mechanism to not only cut off access to these sites and impose operational barriers, 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. Some issues related to online infringement are complex and will require more complex solutions. But some of these issues are clearly right or wrong. Websites that egregiously violate the law at the expense of American consumers and American workers have no place on the Internet. The responsibility for maintaining the Internet falls upon each user, each service provider, and each business and institution that uses it, operates it, and profits by it. The cost of doing nothing or doing too little is high. I encourage you to put in place the frameworks and policies needed to facilitate and encourage all actors within the Internet ecosystem to take some measure of responsibility for maintaining its integrity and protecting consumers.

## Endnotes

---

1. Robert D. Atkinson, "Comments on the Coordination and Strategic Planning of Federal Efforts Against Intellectual Property Infringement," Information Technology and Innovation Foundation, 2010.
2. Shayerah Ilias and Ian F. Ferguson, "Intellectual Property Rights and International Trade," *Congressional Research Service*, December 2007.
3. Shayerah Ilias and Ian Fergusson, "Intellectual Property Rights and International Trade," *Congressional Research Service*, February 5, 2009.
4. David Price, "An Estimate of Infringing Use of the Internet," Envisional (2011), [http://documents.envisional.com/docs/Envisional-Internet\\_Usage-Jan2011.pdf](http://documents.envisional.com/docs/Envisional-Internet_Usage-Jan2011.pdf).
5. "Background Report on Digital Piracy of Sporting Events," Envisional and NetResult, 2008.
6. While P2P file sharing is dominated by copyright content, some people mistakenly associate P2P only with file sharing networks. However, P2P technology encompasses many types of applications and services from the Skype-to-Skype dialing procedure to video streaming on mainstream websites like CNN. (Note: Skype is not truly a P2P application; it only does session initiation by P2P, the rest is a straight UDP session.)
7. As of November 2009, the Pirate Bay was ranked as 109th and isoHunt was ranked as 187th. "Alexa Top 500 Global Web Sites," web page, ND, <http://www.alexa.com/topsites/global> (accessed Nov. 28, 2009).
8. 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>.
9. Result of author's tests on March 10, 2011.
10. 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>.
11. Mary Madden, "The State of Music Online: Ten Years After Napster," Pew Internet & American Life Project, 2009, <http://www.pewinternet.org/Reports/2009/9-The-State-of-Music-Online-Ten-Years-After-Napster.aspx>.
12. Eliza Krigman, "IP Enforcement Policies Stir Censorship Debate," Tech Daily Dose, October 22, 2010, <http://techdailydose.nationaljournal.com/2010/10/ip-enforcement-policies-stir-c.php>.
13. Stephen Siwek, "The True Cost of Copyright Industry Piracy to the U.S. Economy," Policy Report 189, The Institute for Policy Innovation, September 2007.
14. Ibid.
15. IFPI, IFPI 2008 Digital Music Report, IFPI, 2008, 8, <http://www.ifpi.org/content/library/dmr2008.pdf>.
16. These figures are for direct losses. Stephen Siwek, "The True Cost of Sound Recording Piracy to the U.S. Economy," Policy Report 188, *The Institute for Policy Innovation*, September 2007.
17. Stephen Siwek, "The True Cost of Motion Picture Piracy to the U.S. Economy," Policy Report 186, *The Institute for Policy Innovation*, September 2006.
18. Business Software Alliance, Sixth Annual BSA-IDC Global Software 08 Piracy Study, BSA, May 2009, <http://global.bsa.org/globalpiracy2008/studies/globalpiracy2008.pdf>.
19. "Background Report on Digital Piracy of Sporting Events," Envisional and NetResult, 2008.
20. Ibid.
21. International Intellectual Property Alliance, Special Report 301, February, 2009.
22. Motoko Rich, "Print Books Are Target of Piracy on the Web," New York Times, May 11, 2009, <http://www.nytimes.com/2009/05/12/technology/internet/12digital.html>.

- 
23. Randall Stross, "Will Books Be Napsterized?" *New York Times*, October 3, 2009, <http://www.nytimes.com/2009/10/04/business/04digi.html>.
  24. "Traffic Report: Online Piracy and Counterfeiting," *MarkMonitor*, January 2011.
  25. See Carl Bialik, "Dubious Origins for Drugs, and Stats About Them," *Wall Street Journal*, September 10, 2010, <http://blogs.wsj.com/numbersguy/dubious-origins-for-drugs-and-stats-about-them-990/> and Randall W. Lutter, "Counterfeit Drugs," Testimony before the House Committee on Government Reform, Subcommittee on Criminal Justice, Drug Policy, and Human Resources, November 1, 2005, <http://www.fda.gov/NewsEvents/Testimony/ucml12670.htm>.
  26. "Traffic Report: Online Piracy and Counterfeiting," *MarkMonitor*, January 2011.
  27. Kevin Lewis, "The Fake and the Fatal: The Consequences of Counterfeits," *The Park Place Economists: Vol. 17*, 2009, <http://digitalcommons.iwu.edu/parkplace/vol17/iss1/14>.
  28. *Ibid.*
  29. John Teresko "Fighting the IP Wars," *IndustryWeek.com*, February 1, 2008, [http://www.industryweek.com/articles/fighting\\_the\\_ip\\_wars\\_15605.aspx](http://www.industryweek.com/articles/fighting_the_ip_wars_15605.aspx).
  30. Shayerah Ilias and Ian F. Ferguson, "Intellectual Property Rights and International Trade," Congressional Research Service, December 2007.
  31. "The Truth About Counterfeiting," International Anti-Counterfeiting Coalition, n.d. <http://www.iacc.org/about-counterfeiting/the-truth-about-counterfeiting.php> (accessed March 10, 2011).
  32. For more details, please see 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>.
  33. "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](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/](http://www.upi.com/Top_News/2008/04/21/Woman-accused-of-airport-bomb-threats/UPI-38521208794796/).
  34. 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>.
  35. 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>.
  36. Esguerra, "Censorship of the Internet Takes Center Stage in 'Online Infringement' Bill."
  37. 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>.
  38. 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>.
  39. 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>.
  40. 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>.
  41. Esguerra, "Censorship of the Internet Takes Center Stage in 'Online Infringement' Bill."

- 
42. 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>.
  43. “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](http://cdt.org/files/pdfs/Leahy_bill_memo.pdf).
  44. See Paul Vixie, “Taking Back the DNS,” CircleID, June 30, 2010, [http://www.circleid.com/posts/20100728\\_taking\\_back\\_the\\_dns/](http://www.circleid.com/posts/20100728_taking_back_the_dns/).