RESPONDING TO ONLINE PIRACY: MAPPING THE LEGAL AND POLICY BOUNDARIES

Ann Chaitovitz, Charisma Hampton, Kevin Rosenbaum, Aisha Salem, Tom Stoll and Albert Tramposch[‡]

I. INTRODUCTION

In a landmark 1995 report, the United States Department of Commerce anticipated the great promise of the Internet to improve and enhance our lives.[1] More than fifteen years later, that promise is being realized. The deployment of high-speed networks, coupled with rapidly falling costs of production, has provided access to rich cultural resources around the world, enhanced education, and increased the opportunity for democratic participation in government. The Internet continues to transform the production and distribution of creative works, accelerating the pace of global creativity by allowing ever more creators to produce and disseminate their copyrighted works online and providing benefits for authors, copyright owners, users, and the public at large.[2]

Nonetheless, this rapid growth of Internet use, along with the development of technologies that enable the unauthorized distribution of copyrighted works, has fueled the explosive growth of online copyright piracy.[3] The ability of

---

[‡] Albert Tramposch is the Administrator for Policy and External Affairs at the United States Patent and Trademark Office. Ann Chaitovitz, Charisma Hampton, Kevin Rosenbaum, Aisha Salem, and Tom Stoll are attorneys in the Office of the Administrator for Policy and External Affairs at the United States Patent and Trademark Office. The views expressed in this article are personal observations of the authors and do not reflect the official positions of the U.S. Government.

[1] *See* Bruce A. Lehman & Ronald H. Brown, Information Infrastructure Task Force, Intellectual Property and the National Information Infrastructure: The Report of the Working Group on Intellectual Property Rights 179, 182 (1995), http://commcns.org/vmhMbx.

[2] *See* FCC, CONNECTING AMERICA: THE NATIONAL BROADBAND PLAN 3, 10, 15-7, 58 (2010), http://commcns.org/sCCj9m.

[3] U.S. GOV'T ACCOUNTABILITY OFFICE, GAO-10-423, INTELLECTUAL PROPERTY:

digital products to be reproduced inexpensively and distributed immediately around the world means that virtually every copyright industry is affected by online piracy, including the music, motion picture, television, publishing, and software industries.[4]

Online piracy and counterfeiting on a massive scale have a significant impact on the American economy and consumers. According to the Government Accountability Office (GAO), "[t]he U.S. economy as a whole may grow at a slower pace," and fewer taxes will be collected by the U.S. government due to reduced economic activity.[5] While the estimates of the economic impact of online piracy and counterfeiting are numerous, the precise impact is difficult to determine due to a lack of credible data.[6] Despite this difficulty, "research in specific industries suggest[s] that the problem is sizeable."[7] Beyond the lost revenues of content owners, creators, and the government, online piracy and counterfeiting also raises significant health and safety concerns for American consumers. Unsafe counterfeit medicines available for sale via the Internet, for example, pose a life-threatening risk.[8] Additionally, pirated software "may contain malicious programming code that could interfere with computers' operations or violates users' privacy."[9]

In response to the challenges posed by online piracy and counterfeiting, the Obama Administration has made intellectual property protection and enforcement a high priority. Introducing the Administration's plan to combat online piracy and other forms of intellectual property infringement, Vice President Biden explained that "piracy is theft" and "hurts our economy."[10] Former Department of Commerce Secretary Gary Locke also underscored the Administration's commitment to confronting the challenge of online piracy, noting that, "[t]his isn't just an issue of right and wrong" but "a fundamental issue of America's economic competitiveness."[11]

This article discusses the current "state of play" with respect to the growing threat of online intellectual property infringement. Part II discusses recent

---

OBSERVATION ON EFFORTS TO QUANTIFY THE ECONOMIC EFFECTS OF COUNTERFEITS AND PIRATED GOODS 8 (2010), http://commcns.org/uNEqnm.

[4] *Id.* at 8.

[5] *Id.* at 14.

[6] *Id.* at 15.

[7] *Id.*

[8] *Why Should I Be Concerned About Counterfeit Drugs?*, NAT'L ASS'N OF BOARDS OF PHARMACY, http://commcns.org/sfWLei (last visited Dec. 15, 2011).

[9] U.S. GOV'T ACCOUNTABILITY OFFICE, *supra* note 3, at 11.

[10] Gauthem Nagesh, *White House Unveils Plan to Combat Online Piracy and Counterfeit Goods*, THE HILL (June 22, 2010), http://commcns.org/rSVlp8; Rob Lever, *U.S. Unveils Strategy To Fight Piracy Of Intellectual Property*, INDUSTRY WEEK (June 22, 2010), http://commcns.org/s1Bvj2.

[11] Gary Locke, U.S. Sec'y of Commerce, Remarks at Intellectual Property Enforcement, Belmont University, Nashville, Tennessee (Aug. 30, 2010).

actions to confront online piracy and counterfeiting taken by private parties and the government, and the legal bases for such actions. Part III discusses recent legislative proposals to address online piracy and counterfeiting and the concerns raised by critics of the legislation. While there are no simple solutions to the manifold issues raised, and many recent legal actions and legislative proposals canvassed in this article are controversial, this article concludes that the right policy balance is necessary to ensure that the Internet realizes its full potential as a platform for the lawful distribution of creative works for the benefit of American creators, consumers, and businesses.

II. RECENT RESPONSES TO PIRACY

A. Private Actions

In an effort to address online infringement, some plaintiffs have brought private actions and secured broad remedies to protect their intellectual property interests on the Internet. For instance, in March 2010, apparel designers and manufacturers The North Face and Polo Ralph Lauren filed suit against hundreds of named and unnamed foreign domain operators.[12] The foreign sites, seemingly based in China and operating under names similar to the brand names of the plaintiffs, were used to sell counterfeit North Face and Ralph Lauren goods.[13] The plaintiffs made various claims of trademark infringement, counterfeiting, and deceptive business practices under federal and New York state law, seeking damages as well as equitable relief.[14]

In response, the Southern District Court of New York froze the defendants' U.S. accounts and issued a temporary restraining order enjoining them from conducting business over the infringing sites.[15] However, the domain name operators failed to answer and continued to register more counterfeiting sites.[16] As a result, the court entered a default judgment awarding the plaintiffs $78 million in damages and issued a permanent injunction to stop the defendants, as well as third parties (including ISPs), from using, hosting, or providing

---

[12] The North Face Apparel Corp. v. Fujian Sharing Imp. & Exp. Ltd., No. 10 Civ. 01630 (S.D.N.Y. Oct. 4, 2011). *See also* Anthony V. Lupo, David S. Modzeleski & Eva J. Pulliam, *Counterfeiting: The North Face Apparel Corp. v. Fujian Sharing Import and Export, Ltd.*, 11 E-COMMERCE L. REP., AUG. 2011, at 6, *available at* http://commcns.org/ssA0ZN.

[13] North Face Apparel, No. 10 Civ. 01630.

[14] *Id.*

[15] The North Face Apparel Corp. v. Fujian Sharing Imp. & Exp. Ltd., No. 10 Civ. 01630 (S.D.N.Y. entered Mar. 30, 2010).

[16] *Id.* (contempt order for noncompliance of defendants).

services to the infringing sites.[17]

In December 2010, when the defendants still failed to comply, The North Face and Polo Ralph Lauren sought and were granted a court order for contempt.[18] The Court ordered the domain name registries to disable the defendants' domain names and transfer them to plaintiffs. Additionally, the court instructed third parties, including "ISPs, back-end service providers, web designers, [and] sponsored search engine or ad-word providers" to discontinue and disable service to defendants' websites.[19] In the event that the ISPs hosting the defendants' websites were unresponsive, the court further ordered those "responsible for allocating and/or delegating the IP addresses used by Defendants' websites . . . shall, within three (3) days of being given notice, de-delegate or otherwise deny access to the IP addresses used by those Defendants' websites."[20] Finally, the Court directed ecommerce and auction sites, like eBay, to delete the defendants' accounts and listings.[21]

The court's order was particularly important because it included a provision that allowed the plaintiffs to shut down not only infringing sites already in existence, but also infringing sites that had not yet been discovered or even created.[22] This stipulation directly addressed the difficulties of playing "whack-a-mole" with infringing sites that, once shut down, would simply reopen under different domain names.[23] This issue is oftentimes a lingering problem for plaintiffs, due to the fact that it is cost-prohibitive to seek legal redress each time a new site appears.[24] However, with ongoing authority to give notice of the contempt order to infringing sites and related third parties, the plaintiffs could continually initiate the shut-down and seizure of infringing domains. In fact, The North Face and Polo Ralph Lauren have succeeded in shutting down hundreds of counterfeit sites since their contempt order was issued, a sign that this private remedy has been working to their benefit.[25]

B. "Operation In Our Sites"

As the United States Intellectual Property Enforcement Coordinator (IPEC) Annual Report on Intellectual Property Enforcement explains, the United

---

[17] *Id. See also* Tory Burch LLC v. Yong Sheng Int'l Trade Co., Ltd., No. 10 Civ. 9336 (S.D.N.Y. filed May 13, 2011) (order granting default judgment and permanent injunction).

[18] North Face Apparel, No. 10 Civ. 01630.

[19] *Id.*

[20] *Id.* at 8.

[21] *Id.*

[22] *Id.* at 11.

[23] *Id. See also* Tory Burch, No. 10 Civ. 9336 at 7 (explaining the authority given to Tory Burch, LLC to enjoin future websites created in violation of the order).

[24] Lupo, *supra* note 12, at 6.

[25] *Id.*

States faces a great challenge in online infringement, which hampers consumer trust, damages the economy, and poses health and safety risks. [26] Realizing this, the Federal Government has committed to increasing enforcement as part of its comprehensive approach to combating the growing threat of online counterfeiting and piracy. [27] Accordingly, in June 2010, the National IPR Coordination Center (IPR Center), in conjunction with the Immigration and Customs Enforcement Homeland Security Investigations (ICE) and the Department of Justice (DOJ), initiated "Operation In Our Sites,", a program designed to target counterfeit goods and pirated content distributed over the Internet.[28]

1. Operation In Our Sites Seizures

Since its inception, Operation In Our Sites has resulted in the seizure of 350 domain names.[29] The first sting operation seized nine domain names of websites that offered first-run movies, music, and software.[30] The second

---

[26] *See* U.S. INTELLECTUAL PROPERTY ENFORCEMENT COORDINATOR, 2010 U.S. INTELLECTUAL PROPERTY ENFORCEMENT COORDINATOR ANNUAL REPORT ON INTELLECTUAL PROPERTY ENFORCEMENT 3-6 (Feb. 2011) [hereinafter IPEC ANNUAL REPORT], http://commcns.org/tKv6Md.

[27] *Id.* at 6.

[28] *Id.* at 2.

[29] *See Federal Courts Order Seizure of 150 Website Domains Involved in Selling Counterfeit Goods as Part of DOJ, ICE HSI and FBI Cyber Monday Crackdown,* U.S. DEPARTMENT OF JUSTICE (Nov. 28, 2011), http://commcns.org/rOa0lr. It is important to distinguish between the seizure of domain names and the blocking of websites. Information is transmitted over the Internet using numerical Internet protocol addresses (IP addresses), which are assigned to each of the network of computers that make up the Internet. See Jonathan Weinberg, ICANN and the Problem of Legitimacy, 50 DUKE L.J. 187, 194-198 (2000) (discussing the development of Internet Protocol (IP) and Domain Name Systems (DNS)). A user may enter the IP address of a website on a host computer allowing the user computer to retrieve the website data. *Id.* Because an IP address is a complex series of numbers that is cumbersome for users of the Internet to use and remember, a Domain Name System (DNS) is overlaid onto the Internet. *Id.* The DNS allows users to simply type in the name of the website, and the DNS server does the rest. Every Internet Service Provider (ISP) keeps a list of domain names and the corresponding IP addresses for each, which it stores in its DNS server. *Id.* Each domain name includes a top level domain (TLD), or suffix that identifies the nature of the organization that owns the website (e.g. ".com", ".net", or "org"). *Id.* A company called a "registry" manages all domain names within a given top level domain (TLD). *Id.* When the government seizes a domain name, it seizes the DNS name—and only the DNS name—because that DNS name is the property of the alleged infringer. See discussion infra Part II(B)(2) (discussing the legal basis for seizure). The seizure leaves the IP address and the files that constitute the website itself intact. Internet users can still access the website by typing in the IP address itself.

[30] *"Operation In Our Sites" Targets Internet Movie Pirates, ICE, Manhattan U.S. Attorney Seize Multiple Web Sites for Criminal Copyright Violations*, U.S. IMMIGRATION AND CUSTOMS ENFORCEMENT (June 30, 2010), http://commcns.org/sdaAJi.

seizure, dubbed the "Cyber Monday Crackdown," was executed on the busiest online shopping day of the year (the Monday after Thanksgiving) and targeted domain names linked to 82 websites many of which were alleged to sell counterfeit hard goods and some that were alleged to sell pirated movies, music and software.[31] The third seizure occurred just days before Super Bowl Sunday 2011, resulting in the seizure of ten domain names of websites that featured sports and other pay-per-view events.[32] "Operation Broken Hearted," carried out on Valentine's Day 2011, seized 18 domain names of websites that illegally offered copyrighted and counterfeit trademarked goods.[33] The fifth phase of Operation In Our Sites, executed in late May 2011, seized five domain names of websites that sold counterfeit goods and illegally distributed copyrighted materials.[34] The sixth phase, "Operation Shoe Clerk," seized 16 domain names of websites selling counterfeit goods, including shoes, boots, sneakers, jackets, shirts, hats, and sunglasses.[35] The seventh phase dubbed "Operation Strike Out," resulted in the seizure of 58 commercial websites selling and distributing counterfeit sports paraphernalia.[36] The most recent phase coincided with Cyber Monday 2011, resulting in the seizure of 150 domain names of websites illegally selling and distributing a variety of counterfeit goods and copyrighted works.[37]

Some of the websites targeted in the Operation In Our Sites seizures were alleged to be "linking" websites, which provided links to "cyberlocker" websites containing infringing content, and at least one of the websites was

---

[31] IPEC ANNUAL REPORT, *supra* note 26, at 42; *ICE Seizes 82 Website Domains Involved in Selling Counterfeit Goods as Part of Cyber Monday Crackdown*, U.S. IMMIGRATION AND CUSTOMS ENFORCEMENT (November 29, 2010), http://commcns.org/roXzRA.

[32] *See* Affidavit in Support of Application for Seizure Warrant ¶ 7, United States v. HQ-Streams.com, 11 Mag. 262 (S.D.N.Y Jan. 31, 2011) [hereinafter *HQ-Streams.com Affidavit*]; *New York Investigators Seize 10 Websites that Illegally Streamed Copyrighted Sporting and Pay-Per-View Events*, U.S. IMMIGRATION AND CUSTOMS ENFORCEMENT (Feb. 2, 2011), http://commcns.org/scKyhE.

[33] *Sweetheart, but Fake, Deals Put on ICE, "Operation Broken Hearted" Protects Consumers from Counterfeit Valentine's Day Goods*, U.S. IMMIGRATION AND CUSTOMS ENFORCEMENT (February 14, 2011), http://commcns.org/snieHw.

[34] *ICE Puts the Summer Heat on Counterfeiters, PSA Released Last Month Now Has Nearly 100,000 Views*, U.S. IMMIGRATION AND CUSTOMS ENFORCEMENT (May 25, 2011), http://commcns.org/tkowa6.

[35] *Homeland Security Investigations Brings Counterfeit Designers to Heel*, U.S. IMMIGRATION AND CUSTOMS ENFORCEMENT (July 28, 2011), http://commcns.org/ulhYFS.

[36] *ICE Announces Results of 'Operation Strike Out' Protects Consumers from Counterfeit Sports Paraphernalia on the Internet and on the Streets*, U.S. IMMIGRATION AND CUSTOMS ENFORCEMENT (Oct. 31, 2011), http://commcns.org/soaC1y.

[37] *See* Press Release, Federal Courts Order Seizure of 150 Website Domains Involved in Selling Counterfeit Goods as Part of DOJ, ICE HSI and FBI Cyber Monday Crackdown, U.S. DEPARTMENT OF JUSTICE (Nov. 28, 2011), http://commcns.org/rOa0lr.

alleged to be a cyberlocker that stored infringing content.[38] Since all the domain names seized were websites with ".net," ".com," and ".org," which are top-level domains (TLDs) managed by registries located in the United States, ICE directed the registries to restrain and lock the domain names pending transfer of all right, title, and interest to the United States upon completion of forfeiture proceedings.[39] ICE directed the registries to point the domain names to a particular IP address displaying a web page notifying users that the domain names had been seized.[40] The new web page often provided a public service announcement educating the public about the economic impact of copyright infringement and trademark counterfeiting.[41] However, since ICE seized only the domain names and not the actual websites, it remained possible to access the sites by using their IP addresses.

2. *Legal Basis for ICE's Seizures*

While ICE's actions in Operation In Our Sites have been directed against some of the newest forms of piracy and counterfeiting taking place on the Internet, they have been based on some of the oldest legal remedies and enforcement tools in the Anglo-American legal system.[42] The first of these principles is civil forfeiture. Inherited from the English common law and initially used to seize and forfeit ships and goods in admiralty cases, forfeiture statutes evolved to encompass cases of tax evasion, bootleg liquor and, more recently, illegal drugs.[43] The result is that "contemporary federal and state forfeiture statutes reach virtually any type of property that might be used in the conduct of a criminal enterprise."[44]

With regard to online piracy and infringement, Section 2323 of Title 18 of the United States Code provides for civil seizure and forfeiture of property used in connection with criminal copyright and trademark infringement.[45]

---

[39] *See* Verified Complaint ¶¶ 11, 16, 21, 26, 31, 36, 41, United States v. 7 Domain Names, 10 CV 9203 (S.D.N.Y. filed Dec. 9, 2010); Application and Affidavit for Seizure Warrant ¶¶ 17, 37, 58, 76, 88, *In re* 5 Domain Names, No. 10-2822M (C.D. Cal. filed Nov. 17, 2010); *HQ-Streams.com Affidavit*, *supra* note 32, ¶ 14.

[39] Application and Affidavit for Seizure Warrant ¶¶ 102-104, *In re Rapgodfathers.com*, No. 10-2822M (C.D. Cal. Nov. 17, 2010) [hereinafter *RapGodfathers.com Affidavit*]; *HQ-Streams.com Affidavit*, *supra* note 32, ¶¶ 48-49.

[40] *RapGodfathers.com Affidavit*, *supra* note 39, ¶¶ 102-104; *HQ-Streams.com Affidavit*, *supra* note 32, ¶¶ 48-49.

[41] *See ICE Puts the Summer Heat on Counterfeiters*, *supra* note 34.

[42] Robert Lieske, *Civil Forfeiture Law: Replacing the Common Law with a Common Sense Application of the Excessive Fines Clause of the Eighth Amendment*, 21 WM. MITCHELL L. REV. 265, 271-281 (1995).

[43] *See* J.W. Goldsmith, Jr.-Grant Co. v. United States, 254 U.S. 505, 508-11 (1921).

[44] Calero-Toledo v. Pearson Yacht Leasing Co., 416 U.S. 663, 683 (1974).

[45] 18 U.S.C. § 2323(a)(1) (2006).

Although Section 2323 was added by Section 206(a) of the Prioritizing Resources and Organization for Intellectual Property Act of 2008, its provisions were not entirely new.[46] The congressional record of the 2006 Stop Counterfeiting in Manufactured Goods Act highlights the fact that Congress was aware that bad actor websites might be seized under the new law. Specifically, Senator Patrick Leahy of Vermont noted that:

> [Current law] cannot be used to pursue forfeiture and seizure proceedings against the computer equipment, website or network of responsible Internet marketplace companies, who serve solely as a third-party to transactions and do not tailor their services or their facilities to the furtherance of trafficking or attempts to traffic in counterfeit marks. . . Companies must establish and implement procedures to take down postings that contain or offer to sell goods, services, labels, and the like in violation of this act upon being made aware of the illegal nature of these items or services. It is the irresponsible culprits that must be held accountable.[47]

Section 2323 also incorporates the procedures of the Civil Asset Forfeiture Reform Act of 2000 ("CAFRA").[48] Under this statute, a seizure may take place only after the government obtains a warrant under the standard procedures of the Federal Rules of Criminal Procedure.[49] Accordingly, an affidavit or sworn testimony must be submitted to a neutral magistrate, establishing probable cause to believe that the property is subject to forfeiture.[50] During seizures under Operation In Our Sites, ICE acted based on probable cause that the domain names were property used or intended to be used to commit or facilitate criminal copyright infringement.[51] Thus, the domain names were subject to seizure and forfeiture pursuant to Section 2323.[52]

Under this process, ICE must provide written notice to interested parties "as soon as practicable" after the date of the seizure or else file a judicial forfeiture

---

[46] *See* Prioritizing Resources and Organizations for Intellectual Property Act of 2008, Pub. L. No. 110-403, 122 Stat. 4262 (2008). Among other things, the PRO-IP Act re-organized forfeiture provisions that had been added by the 2006 Stop Counterfeiting in Manufactured Goods Act. *See id*; Stop Counterfeiting in Manufactured Goods Act, Pub. L. No. 109-181, 120 Stat. 288 (2006) (codified in scattered sections of 17 & 18 U.S.C.).

[47] 151 CONG. REC. 25798 (Nov. 10, 2005) (statement of Sen. Patrick Leahy).

[48] 18 U.S.C. §§ 981-987 (2006 & Supp. 2010).

[49] *See* 18 U.S.C. § 981(b)(2).

[50] *See* Fed. R. Crim. P. 41(d)(1)-(2).

[51] *See* 17 U.S.C. § 506(a)(1)(c) (2006) (prohibiting criminal copyright infringement, including *inter alia* willfully infringing a copyright "by making it available on a computer network accessible to members of the public"); 18 U.S.C. § 2319 (providing punishments for violations of 17 U.S.C. § 506(a)).

[52] *See RapGodfathers.com Affidavit*, *supra* note 39 ¶ 4; *HQ-Streams.com Affidavit*, *supra* note 32 ¶ 5; Verified Complaint at 15, United States v. TVShack.net, No. 10 CV 9203 (S.D.N.Y. Dec. 9, 2010). While the law is not settled regarding whether a domain name constitutes property subject to seizure, the Ninth Circuit Court of Appeals has held that a property right exists in a domain name because it represents an interest of precise definition, is subject to exclusive possession of control, and a registrant has a legitimate claim to exclusivity in a domain name. *See* Kremen v. Cohen, 337 F.3d 1024, 1030 (9th Cir. 2003).

action against the property.[53] The domain name owner then has the right to file an administrative claim for the property seized by the deadline set in the notice.[54] Within 90 days of the filing of domain name owner's administrative claim, the government must file a judicial forfeiture complaint or include the property in a criminal indictment.[55] More than half of the websites seized have been administratively forfeited.[56] Failure to do so requires the immediate release of the domain name to the claimant, so long as it is unlikely to be used for additional crimes and the hardship from the seizure outweighs the risk that the domain name will be damaged, lost, destroyed, concealed or moved.[57] If the property has not been released within 15 days of the administrative claim filing, the claimant may petition the district court in which the seizure warrant was issued.[58]

3. *Legal Issues and Challenges with Seizures*

One complaint with Operation In Our Sites is that the lack of an adversarial procedure before a domain name is seized deprives the domain name owners of due process. Congresswoman Zoe Lofgren, a long-time opponent of Operation In Our Sites, stated that "domain seizures without due process are a form of censorship. . . . While this might be enough for the seizure of stolen cars or knock-off handbags, it is not enough for websites and speech on the Internet."[59] Additional critics argue that the absence of a full adversarial hearing presents an increased risk of improper seizure.[60] David Sohn of the

---

[53] 18 U.S.C. § 983(a)(1)(A)(i)-(ii).

[54] *Id.* § 983(a)(2).

[55] *Id.* § 983(a)(3).

[56] According to ICE, 65 of 120 domain names ICE has seized have been administratively forfeited as of April 26, 2011. *See* Press Release, New Public Service Announcement Launched to Raise Intellectual Property Theft Awareness, U.S. IMMIGRATION AND CUSTOMS ENFORCEMENT (Apr. 26, 2011), http://commcns.org/veLw2N.

[57] 18 U.S.C. § 983(f)(1), (f)(8)(D) (an example of a hardship under the statute would be preventing a business from functioning, preventing an individual from working, or leaving an individual homeless).

[58] *Id.* § 983(f)(3). To date, at least one owner of a seized domain name has filed a petition with a district court under 18 U.S.C. Section 983(f) for release of the seized domain name. Memorandum of Points and Auth. in Support of Puerto 80's Petition for Release of Seized Prop. and in Support of Request for Expedited Briefing and Hearing of Same at 6, Puerto 80 Projects, S.L.U. v. United States, No. 11 Civ. 3983 (S.D.N.Y. 2011), *appeal granted*, No. 11-3390 (2d Cir. Aug. 19, 2011).

[59] Rep. Zoe Lofgren, *Lofgren, Wyden Question Response to Seizure Inquiries*, http://commcns.org/tyiKZR (last visited Dec. 15, 2011).

[60] *Promoting Investment and Protecting Commerce Online: Legitimate Sites v. Parasites, Part I: Hearing Before the H. Comm. on the Judiciary, Subcomm. on Intellectual Property, Competition, and the Internet*, 112th Cong. 6-9 (2011) [hereinafter *Online Commerce Hearing I*] (statement of David Sohn, Senior Policy Counsel, Center for Democracy &

Center for Democracy & Technology (CDT) has noted that in such instances, "mitigating factors and overbreadth issues may not come to light before the name is seized or blocked. In a one-sided process, the risk of mistakes or overaggressive action is high."[61]

Supporters of Operation in Our Sites believe there is no greater risk of error in seizing domain names than there is in seizure of other types of personal property.[62] In fact, since the content and servers are still available to the owner and the website can still be accessed via the IP address, supporters maintain that the risk of error for seizure of domain names is actually *less* than in seizures of other personal property.[63] These proponents also distinguish between domain name seizure and forfeiture; while seizure is the act of taking custody of property, forfeiture involves the involuntary relinquishment of property as a consequence of the commission of a crime.[64] Additionally, as the Supreme Court has held, notice and hearing *after* the property is seized satisfies due process when that property is seized "to secure an important governmental or general public interest."[65]

ICE repeatedly has noted that the Operation In Our Sites domain name seizures are conducted as part of criminal investigations after judicially authorized seizure warrants are obtained.[66] As ICE Director John Morton highlights:

> Domain names seized under Operation In Our Sites are seized only in furtherance of ongoing criminal investigations into violations of U.S. federal laws. . . . For each domain name seized, ICE investigators independently obtained counterfeit trademarked goods or pirated copyrighted material that was in turn verified by the rights holders as counterfeit. After such verification, ICE applied for federal seizure warrants based on probable cause. Federal magistrate judges approve criminal seizure warrants based on probable cause for the domain names that are targeted. The standard is exactly the same as in any other criminal investigation. As with all judicially authorized seizure warrants, the owners of the seized property have the

---

Technology), http://commcns.org/sCSXbA.

[61] *Id.* at 7.

[62] Terry Hart, *Feds Seize Domain Names*, COPYHYPE (Dec. 6, 2010), http://commcns.org/vAUtBq. *See also* John A. Greer, *If the Shoe Fits: Reconciling the International Shoe Minimum Contacts Test with the Anticybersquatting Consumer Protection Act*, 61 VAND. L. REV. 1861, 1885-88 (2008) (noting that domain names should be characterized as property and thus subject to property law).

[63] *See Feds Seize Domain Names*, *supra* note 62 (arguing that seizure of domain names has a lower risk of error than other types of property seizures).

[64] Larry Downes, *Domain Name Seizures and the "Limits" of Civil Forfeiture,* THE TECHNOLOGY LIBERATION FRONT (Nov. 29, 2010), http://commcns.org/vpKty9.

[65] Calero-Toledo v. Pearson Yacht Leasing Co., 416 U.S. 663, 676-80 (1974) (quoting Fuentes v. Shevin, 407 U.S. 67, 91 (1972)).

[66] Letter from John Morton, Assistant Secretary U.S. Immigration and Customs Enforcement, Department of Homeland Security, to Zoe Lofgren, Member, U.S. House of Representatives (May 9, 2011), http://commcns.org/tmQRlx.

opportunity to challenge the judge's determination through a petition.[67]

In the same way that "law enforcement agencies do not notify suspects of impending criminal enforcement actions prior to their execution," ICE argues that there is no reason to notify the owners of domain names prior to seizure for suspected violations of criminal copyright and trademark laws.[68]

Critics of Operation in Our Sites also raise First Amendment concerns in connection with ICE's seizures. They argue that seizing domain names of websites that allegedly contain infringing or counterfeit material violates the First Amendment by imposing a prior restraint on protected speech and affecting lawful speech in a number of ways.[69] Specifically, since Operation In Our Sites targets entire domains, these seizures may affect a combination of "lawful and unlawful content, including non-Web content like email or instant messaging connections."[70] Furthermore, the existence of subdomains is particularly troubling, because "[m]any web hosting services are constructed in a way such that thousands of individual sites, created and maintained by thousands of individuals, share a single domain name."[71] As a result, should Operation In Our Sites target one of these domain names, the seizure would affect the entire platform, not just the actual targeted offenders.[72]

Some supporters of ICE's actions compare domain name seizures to the confiscation of obscene materials, thereby concluding that Operation In Our Sites fits within the boundaries of the First Amendment.[73] Specifically, the government must clear two particular hurdles for a seizure of allegedly obscene material to be found constitutional.[74] First, the seizure warrant must describe the targeted material with specificity.[75] In the case of domain names,

---

[67] *Promoting Investment and Protecting Commerce Online: Legitimate Sites v. Parasites, Part II: Hearing Before the H. Comm. on the Judiciary, Subcomm. on Intellectual Property, Competition, and the Internet*, 112th Cong. 11-12 (2011) [hereinafter *Online Commerce Hearing II*] (statement of John Morton, Director of U.S. Immigration and Customs Enforcement, Department of Homeland Security), http://commcns.org/t38zzN.

[68] Letter from John Morton, Director of U.S. Immigration and Customs Enforcement, Department of Homeland Security, to Zoe Lofgren, Member, U.S. House of Representatives (May 9, 2011), http://commcns.org/tmQRlx. *See also Online Commerce Hearing II*, *supra* note 67, at 4 (statement of John Morton, Director of U.S. Immigration and Customs Enforcement, Department of Homeland Security).

[69] *Online Commerce Hearing I*, *supra* note 60, at 9 (statement of David Sohn, Senior Policy Counsel, Center for Democracy & Technology).

[70] *Id.* at 6.

[71] *Id.* at 8.

[72] *Id.* at 8-9 (discussing the recent example of "mooo.com" seizure under Operation Protect Our Children, and stating that the tactics used by ICE were not narrowly tailored to the criminal actors).

[73] *Feds Seize Domain Names*, *supra* note 62 (noting that "[t]he law requires certain procedural safeguards to protect against the abridgement of speech rights.").

[74] *See id. See also* U.S. CONST. amend. IV.

[75] *See Feds Seize Domain Names*, *supra* note 62. *See also* Stanford v. Texas, 379 U.S.

the government met this constitutional requirement because "the seizures were made pursuant to valid, specific warrants issued by a neutral, impartial judge."[76] Second, the government must obtain a judicial determination in order to impose a final restraint on speech.[77]

Proponents argue that the seizure of domain names is not a final restraint because "the purpose of seizing these domain names is to establish and preserve *in rem* jurisdiction for forfeiture proceedings." [78] Since users can still access the site by its IP address and the site owner is not prevented from setting up a new domain name, the seizure does not amount to a form of censorship.[79]

Responding to criticism that its actions harmed websites that facilitated legitimate, non-infringing speech, ICE stated that:

> All of the domain names seized through court orders obtained during Operation In Our Sites were commercial sites, profiting from criminal trademark violations and criminal copyright infringement through a combination of sales, advertising revenue, and subscription fees. As a law enforcement agency, ICE has no interest in disrupting lawful commerce or protected speech.[80]

ICE has also noted that it worked closely with the Department of Justice to review "the existence, or lack thereof, of constitutionally protected speech on each website" before undertaking any of its seizures.[81]

The last issue critics raise in connection with Operation In Our Sites is the federal government's jurisdiction over foreign websites and associated domain names. While some argue that the U.S. government maintains jurisdiction over these sites because their domain names are registered in the U.S., others regard this nexus as insufficient,[82] pointing out that, without a single jurisdiction, individuals may be subject to prosecutions from a number of different countries.[83]

ICE has recognized that many of the targeted websites are operated and

---

476, 485 (1965); U.S. CONST. amend. IV.

[76] *Feds Seize Domain Names*, *supra* note 62.

[77] *Id. See also* Heller v. NY, 413 U.S. 483, 489 (1973). A final restraint would include, for example, being enjoined from using a particular domain name.

[78] *Feds Seize Domain Names*, *supra* note 62 (critics to this argument respond that, unlike real property, there is no need to preserve the jurisdiction or possession of domain names registered in the U.S., as there is no risk of flight).

[79] *Id.*

[80] Letter from John Morton, Assistant Secretary, U.S. Immigration and Customs Enforcement, to Zoe Lofgren, Member, U.S. House of Representatives, at 4 (May 9, 2011), *available at* http://commcns.org/tmQRlx.

[81] *Id.*

[82] Peter Walker, *US Anti-piracy Body Targets Foreign Website Owners for Extradition: Britons Could Face Charges for Breaking US Copyrights Even if They Have No Link to America and Servers Are Based Elsewhere*, THE GUARDIAN (July 3, 2011), http://commcns.org/vlOSCj. (quoting Jim Killock, executive director of the Open Rights Group).

[83] *Id.*

hosted in foreign countries that do not have positive working relationships with U.S. law enforcement.[84] Since there may be no known physical assets in the United States associated with these sites, "seizure of a domain name that is registered in the United States is the sole law enforcement action available."[85] Further justifying its jurisdiction, ICE notes that it investigates copyright and trademark violations "only when there is a U.S. nexus, such as a U.S. copyright or trademark being violated or an obvious intent to sell counterfeit goods to American consumers."[86] The test is whether a website is "actively used to violate U.S. laws."[87]

In a recent interview, Victoria Espinel, the U.S. IPEC, insisted that the goal of asserting jurisdiction over these foreign websites is to protect American citizens.[88] Even if global operations cannot be contained, these seizures restrict the access of these sites to the U.S. market.[89] However, since the law used in Operation in Our Sites provides jurisdiction only over websites that have TLDs registered in the U.S., many foreign rogue websites that target U.S. consumers and harm U.S. copyright owners remain out of reach.[90]

4. *Case Study: Rojadirecta*

In order to understand the practical effect of Operation In Our Sites, it is helpful to study the experience of Rojadirecta. To date, this is the only case in which the domain name owner has filed a petition for the release of its seized domain name.[91] The owner, Puerto 80 Projects ("Puerto 80"), registered its Rojadirecta domain names with GoDaddy.com, Inc., a U.S. company, despite having a principal place of business in Arteixo, Spain.[92] According to ICE, Rojadirecta was a "linking" website that "collected and catalogued links to

---

[84] Letter from John Morton, Assistant Secretary, U.S. Immigration and Customs Enforcement, to Zoe Lofgren, Member, U.S. House of Representatives, at 6 (May 9, 2011), *available at* http://commcns.org/tmQRlx.

[85] *Id.*

[86] *Id.* at 7.

[87] *Id.*

[88] Ben Sisario, *Interview With the U.S. Copyright Czar*, N.Y. TIMES (June 8, 2011), http://commcns.org/tMeROl.

[89] *Id.*

[90] Margaret Grazzini, *Four Rounds of ICE Domain Name Seizures and Related Controversies and Opposition*, BERKELEY TECH. L.J. BOLT (Feb. 23, 2011), http://commcns.org/sme6xO.

[91] *See generally* Puerto 80 Memorandum, *supra* note 58. *See also* David Kravets, *Feds Defend Internet Domain Seizure in Piracy Crackdown*, WIRED (July 12, 2011), http://commcns.org/t8LNOe; Dan Goodin, *Site Appeals Feds' Unprecedented Domain Seizure*, THE REGISTER (June 14, 2011), http://commcns.org/rUnGF3.

[92] Puerto 80 Memorandum, *supra* note 58, at 2 (Puerto 80 had condensed both rojadirecta.com and rojadirecta.org into a single website known as "Rojadirecta").

files on third-party websites that contained illegal copies of copyrighted content," specifically live and previously aired sporting and pay-per-view events.[93] In signing the seizure warrant subsequently executed by ICE, the Southern District of New York found probable cause to believe that the domain names had been used to commit criminal violations of copyright law, and therefore were subject to forfeiture.[94]

As previously explained, a number of requirements must be met before property can be released.[95] Puerto 80 argued that, at the time of its petition, the Rojadirecta website had experienced a 32% reduction in online traffic as a result of the seizure and that continued possession of the domain names would "substantially and irreparably harm the goodwill of the Rojadirecta site and drive its customers away."[96] Puerto 80 also argued that the seizure of its domain names constituted an unlawful prior restraint on its users' protected speech under the First Amendment, imposing a further hardship under the statute.[97] Finally, Puerto 80 argued that the Rojadirecta linking material did not constitute direct copyright infringement.[98] In support, CDT, the Electronic Frontier Foundation (EFF), and Public Knowledge argued that the seizure of the Rojadirecta domain names violated both the substantive and procedural requirements of the First Amendment[99] and disregarded "important international norms" by ignoring the judgment of two Spanish courts that found Puerto 80 not liable for copyright infringement.[100]

The District Court disagreed, holding that Puerto 80 did not meet the requisite "substantial hardship" under the statute[101] The Court first pointed to the fact that Rojadirecta had already transferred its website to alternative domain names beyond the jurisdiction of the United States government that could be found easily by the website's users.[102] The claimed reduction in visitor traffic was therefore not enough to establish a substantial hardship.[103]

---

[93] Memorandum of Law in Opposition to Petition of Puerto 80 Projects Seeking Release of Seized Property at 4, Puerto 80 Projects, S.L.U. v. United States, No. 11 Civ. 3983 (S.D.N.Y. 2011), *appeal granted*, No. 11-3390 (2d Cir. Aug. 19, 2011).

[94] Puerto 80 Projects, S.L.U. v. United States, No. 11 Civ. 3983, slip op. at 1 (S.D.N.Y. Aug. 4, 2011), *appeal granted*, No. 11-3390 (2d Cir. Aug. 19, 2011).

[95] *See* discussion, *supra* Part II.B.2.

[96] Puerto 80 Memorandum, *supra* note 58, at 9.

[97] *Id.* at 10-12.

[98] *Id.* at 15-16.

[99] Brief for Electronic Frontier Foundation et al. as Amici Curiae Supporting Plaintiff at 7-13, Puerto 80 Projects, S.L.U. v. United States, No. 11 Civ. 3983 (S.D.N.Y. 2011), *appeal granted*, No. 11-3390 (2d Cir. Aug. 19, 2011).

[100] *Id.* at 13.

[101] Puerto 80 Projects, S.L.U. v. United States, No. 11 Civ. 3983, slip op. at 3-4 (S.D.N.Y. Aug. 4, 2011).

[102] *Id.* at 3.

[103] *Id.* at 4.

The Court also rejected Puerto 80's First Amendment challenge, stating that "the main purpose of the Rojadirecta websites . . . is to catalog links to . . . copyrighted athletic events," not for any discussions that may take place in fora on the site.[104] As a result, "the fact that visitors must now go to other websites to partake in the same discussions is clearly not the kind of substantial hardship Congress intended to ameliorate in enacting § 983."[105]

Since the Court found no substantial hardship, it declined to discuss whether Puerto 80 would use the domain names to commit additional criminal acts if the petition were granted and the domain names were released.[106] Puerto 80 has since appealed the decision to the United States Court of Appeals for the Second Circuit.[107]

III. POSSIBLE PATHS FORWARD

The Obama Administration, Congress, the states, business and labor also have made stopping online infringement a high priority because of the significant harm intellectual property theft causes the U.S. economy and the threat it poses to American businesses and jobs. For example, in a letter to the chairs and ranking members of the Senate and House Judiciary Committees, 42 state attorneys general from the National Association of Attorneys General voiced concern that criminals have turned to the Internet to make incredible profits while rogue websites based overseas are presenting law enforcement with difficult enforcement challenges.[108] On this issue, business and labor agree that government assistance is needed to combat these threats. In a letter dated February 15, 2011, 130 companies and labor organizations asked Congress to take action to stop rogue websites from hurting their businesses by selling counterfeit and pirated products.[109] Although the harm to U.S. jobs and the economy is difficult to quantify, no one disputes that online piracy harms a number of important industries, including software, gaming, movie, music, clothing, luxury goods and countless other industries.[110]

---

[104] *Id.*

[105] *Id.*

[106] *Id.* at 5.

[107] Order Granting Puerto 80's Unopposed Motion to Expedite Its Appeal, Puerto 80 Projects, S.L.U. v. United States (2nd Cir. 2011) (No. 11-3390-cv).

[108] Letter from the National Association of Attorneys General to the Senate and House Judiciary Committees (May 16, 2011), *available at* http://commcns.org/skoDIv.

[109] See Letter from Businesses and Professional and Labor Organizations to Members of Congress (Feb. 15, 2011), *available at* http://commcns.org/rCIBqC. *See also* Juliana Gruenwald, Groups Urge Action On Bill To Combat Online Piracy, NAT'L J. (Feb. 15, 2011), http://commcns.org/v7Impq.

[110] Press Release, Senator Patrick Leahy, Leahy, Hatch, Grassley Unveil Targeted Bill To Counter Online Infringement (May 12, 2011), http://commcns.org/ux8GBg; Press Release,

While DOJ and ICE have worked to quell the threats to American industry, law enforcement agencies have found that existing law leaves little recourse for stopping foreign owned and operated websites from stealing U.S. intellectual property and selling it to U.S. consumers online.[111] Thus far, Congress and the Administration have attempted to resolve the problem a number of ways, including publishing lists of infringing sites to shame countries into reining in rampant online infringement originating within their borders.[112] Nevertheless, these efforts have not been enough to stop online piracy originating overseas in foreign rogue websites.

A. How Recent Legislative Proposals Attempt to Address the Problem

Congress recently drafted legislation to bridge the gap between ICE's ability to institute civil forfeiture proceedings against domestic domain names and its inability to combat piracy on websites that do business in the U.S., but are registered and operate in foreign countries. On September 2010, Senator Patrick Leahy and other members of the Senate Judiciary Committee introduced the Combating Online Infringement and Counterfeits Act (COICA) to supplement the existing legal arsenal to combat the problem of foreign websites that make infringing content available to U.S. users.[113] However, despite Judiciary Committee passage in November 2010, and several hearings on the bill, COICA never received a full Senate vote.[114]

As a result, in the next Congress, Senator Leahy again amassed a bipartisan group of senators in the 112th Congress[115] to introduce a revised bill, known as the Preventing Real Online Threats to Economic Creativity and Theft of

---

Sen. Patrick Leahy, Senators Introduce Bipartisan Bill To Combat Online Infringement (Sept. 20, 2010), http://commcns.org/sz4K3r. *See also* BUSINESS SOFTWARE ALLIANCE, 2010 GLOBAL SOFTWARE PIRACY STUDY (May 2011), http://commcns.org/uCmdxm (estimating that $59 billion dollars' worth of software was used illegally last year worldwide).

[111] Press Release, Sen. Patrick Leahy, Senators Introduce Bipartisan Bill To Combat Online Infringement (Sept. 20, 2010), http://commcns.org/sz4K3r.

[112] *See* U.S. CONGRESS, THE CONGRESSIONAL INTERNATIONAL ANTI-PIRACY CAUCUS, 2011 COUNTRY WATCH LIST (2011), http://commcns.org/slubP3; U.S. TRADE REPRESENTATIVE, OUT-OF-CYCLE REVIEW OF NOTORIOUS MARKETS, http://commcns.org/u8S5rj (Feb. 28, 2011).

[113] *See* Combating Online Infringement and Counterfeits Act, S. 3804, 111th Cong. 4-6 (2010).

[114] Nate Anderson, *Senator: Web Censorship Bill A 'Bunker-Busting Cluster Bomb'*, WIRED (Nov. 20, 2010), http://commcns.org/u7cCI9; Stephen C. Webster, *Oregon Senator Wyden Effectively Kills Internet Censorship Bill,* THE RAW STORY (Nov. 19, 2010), http://commcns.org/sFaEbL.

[115] Press Release, Sen. Patrick Henry, Senate Judiciary Committee Unanimously Approves Bipartisan Bill To Crack Down on Rogue Websites (May 26, 2011), http://commcns.org/urZNAr.

Intellectual Property Act ("PIPA" or "PROTECT IP Act").[116] PIPA shared COICA's goal of providing a mechanism for law enforcement to combat counterfeiting and piracy in the U.S. by enabling recourse against foreign sites operating in the U.S. whose sole purpose is to profit from infringement of the intellectual property rights of others.[117] On May 26, 2011, the Senate Judiciary Committee reported PIPA out of Committee.[118]

The following sections compare the major portions of both COICA and PIPA, addressing the threshold requirements for action, jurisdictional limitations and authority granted to the Attorney General, and private rights holder actions. These sections distinguish the financial transaction provider and advertising services provisions of both COICA and PIPA, their potential extraterritorial impact, and related Internet security concerns. Finally, the article addresses the major First Amendment and Due Process criticisms of COICA and highlights how PIPA deals with these concerns.

1. Authorized Actions Under COICA and PIPA

Both COICA and PIPA provide a different basis for actions against infringing sites. Instead of seizure and forfeiture of domain names, as used in Operation in Our Sites, the new legislation provides equitable remedies against domain names to cease and desist from undertaking any further infringing activities. Therefore, under the proposed legislation, no property is ever seized or forfeited, but rather temporary restraining orders, preliminary injunctions, and injunctions are directed against infringing domain names. The statutes incorporate the protections of the Federal Rules of Civil Procedure as well.

COICA provided the DOJ with an expedited process for cracking down on foreign rogue Internet sites and disrupting criminal enterprises operating online by targeting the domain names "dedicated to infringing activities."[119] Under the COICA definition, an Internet site was dedicated to infringing activities if it met one of two prongs. The first required it to be subject to civil forfeiture as a result of criminal infringement under 18 U.S.C. § 2323.[120] Alternatively, a website could meet this standard if it is primarily designed or marketed to offer infringing goods and services or counterfeit products, or has no demonstrable commercially significant purpose, and engaged in criminal infringement, and when taken together, those activities are the central activities of the Internet

---

[116] Preventing Real Online Threats to Economic Creativity and Theft of Intellectual Property Act of 2011, S. 968, 112th Cong. (2011).

[117] *See id.*

[118] Mike Palmedo, *PROTECT IP Act Clears Sen. Judiciary Committee—Sen. Wyden Places a Hold on Bill*, INFOJUSTICE (May 27, 2011), http://commcns.org/uKduLL.

[119] *See* S. 3804 § 2(a)(1)(A).

[120] *See id.* § 2(a)(1)(A).

site accessed through the domain name that is the subject of the action.[121]

This definition set a high threshold for sites that could be targeted under the legislation. Particularly, only sites subject to civil forfeiture for criminal copyright infringement would be subjected to domain name disabling. Critics of COICA, however, expressed concerns that its implementation would censor websites, harm innovation on the Internet, and run afoul of the fair use doctrine in copyright law and the First Amendment.[122] PIPA has attempted to rectify some of those concerns revising the definition of an "Internet site dedicated to infringing activities." Under PIPA, such a site that "has no significant use other than engaging in, enabling, or facilitating" (1) the infringement of copyrighted works in complete or substantially complete form; (2) the circumvention of copyright protection systems; or (3) the sale of goods, services, or materials bearing a counterfeit mark.[123] The definition also includes Internet sites "designed, operated, or marketed by its operator, primarily as a means for engaging in, enabling or facilitating the acts described above."[124]

Rather than including websites that accidentally distribute infringing goods, PIPA focuses more narrowly on sites that have "no significant use other than the engaging, enabling, or facilitating" the infringing activity, which allows it to target only the most egregious infringers.[125] Therefore, if a website makes available or distributes infringing goods, but that distribution is incidental to the site's viable, legal commercial purpose, it would not be targeted under PIPA. Conversely, a website that exists solely to sell or distribute illegal copies of protected works would fall within the scope of the legislation. These websites are deemed the "worst of the worst" because they appear authentic and are easily accessible by entering domain names that sound legitimate, but exist instead to exploit and misappropriate the intellectual property of others.[126]

COICA and PIPA do not provide jurisdiction over foreign businesses based on their overseas business, but rather jurisdiction is based on a foreign businesses' contacts with U.S. consumers.[127] As in COICA, under PIPA, injunctions can only be issued against sites dedicated to infringing activity if: (1) the domain name is used within the U.S. to access the site; (2) the site conducts business directed to U.S. residents; and 3) the site harms holders of

---

[121] *Id.* § 2(a)(1)(B)(i).

[122] Declan McCullagh, *Senate Panel Approves Domain Name Seizure Bill*, CNET NEWS (Nov. 18, 2010), http://commcns.org/tqM8HF.

[123] *See* S. 968 § 2(7)(A)(i)-(iii).

[124] *Id.* § 2(7)(B).

[125] *Id.* § 2(7)(A).

[126] S. REP. NO. 112-39, at 3, 9 (2011).

[127] *See generally* S. 3804 and S. 968.

U.S. IP rights.[128] The legislation directs courts to look to a variety of factors to make this determination, including whether the site provides goods or services to U.S.-based users, offers services obtained in the U.S., and offers goods or services for sale in U.S. dollars. Additionally, the court must examine whether there is evidence that the site does not intend to provide, or has reasonable measures in place to prevent, access to or delivery of infringing goods or services to users located in the U.S.[129]

COICA authorized the Attorney General to bring an *in rem* action and seek injunctive relief against any domain name used by sites with a domestic or international registry or registrar if the site was dedicated to infringing activities.[130] Following commencement of the *in rem* action, and upon application of the AG, COICA authorized a court, in accordance with Rule 65 of the Federal Rules of Civil Procedure, to issue a temporary restraining order, preliminary injunction, or injunction against the domain name.[131] If the action was against a domestic domain name, the injunction could be served on the registry or registrar; if the site had a foreign registrar or registry, the injunction could be served on service providers, financial transaction providers, and advertising services.[132]

PIPA authorizes the AG and individual rights holders to commence civil actions and seek injunctive relief against (1) a registrant of a domain name used by a site dedicated to infringing activities; (2) the owner or operator of an site dedicated to infringing activities; or (3) the domain name itself (pursuant to an *in rem* action).[133] Upon application of the AG or an individual rights holder following the commencement of the action, a court is authorized, in accordance with Rule 65 of the Federal Rules of Civil Procedure, to order the entity against whom the action was commenced to cease and desist from undertaking any further infringing activity.[134] These orders may be served on the operators of non-authoritative domain name servers, financial transaction providers, Internet advertising services, and information location tools.[135] It is important to note that PIPA authorizes a court to issue an injunction against operators of non-authoritative domain name services and information location tools only in AG actions against nondomestic domains; private rights holders

---

[128] S. 968 §§ 3(b)(1)(A)-(B), 4(b)(1)(B).
[129] *See id.* §§ 3(b)(2), 4(b)(2).
[130] S. 3804 § 2(b)-(d) (2010).
[131] *Id.* § 2(b) (2010).
[132] *Id.* § 2(e)(1)-(2) (2010).
[133] *See* S. 968, §§ 3(a)(1)-(2), 4(a)(1)-(2). The terms "domain name," "internet site," and "internet site dedicated to infringing activities," are separately defined in § 2 of the bill. *See id.* §§ 2(1), (6)-(7).
[134] *See id.* §§ 3(b)(1), 4(b)(1)-(2).
[135] *Id.* §§ 3(d)(1), 4(d)(1).

are denied an injunction against these entities.

2. "Indirect Enforcement": Financial Transaction Provider and Advertising Services Provisions

Both the DOJ and individual rights holders face obstacles when confronting and deterring rogue websites dedicated to infringing activities directed at American consumers. Operators of rogue websites are difficult to target directly and can often act with relative impunity.[136] These websites operate with the appearance of legitimacy, in part, because they often accept payment for their infringing wares through established credit card companies, banks, and related payment processing entities.[137] Additionally, advertisements for legitimate products and services appear on these website, providing an important source of revenue for the operators.[138] Paid advertisements or sponsored links for rogue websites also frequently appear in search engine results, and as a result, such advertisements readily reach American consumers.[139] Problems like these have prompted legislation aimed at cutting off such revenue streams to rogue websites and include provisions to secure cooperation from third party entities like financial transaction providers and Internet advertising services.[140]

---

[136] *See* S. REP. NO. 112-39, at 3-4 (2011) ("[B]ecause this theft is veiled by the complexities of the online world and many of the perpetrators are located overseas, the task of enforcing U.S. intellectual property laws on the Internet is a difficult one."); *Targeting Websites Dedicated to Stealing American Intellectual Property: Hearing Before the S. Comm. on the Judiciary*, 112th Cong. 2 (2011) [hereinafter *IP Theft Hearing*] (statement of Tom Adams, Chief Executive Officer, Rosetta Stone Inc.), http://commcns.org/seDQGM (testifying that Rosetta Stone's customer care department receives calls from U.S. consumers who have mistakenly purchased pirated products over the Internet and that most of the purchases are made from rogue websites "based in China, Russia and other foreign countries, beyond the reach of U.S. law enforcement").

[137] *See* S. REP. NO. 112-39, at 3-4 (2011) (counterfeiters' websites appear legitimate, in part, because, "they often accept payment through well respected credit card companies").

[138] *See id.* (to appear legitimate, counterfeiters' websites "often run advertisements from trusted companies").

[139] *IP Theft Hearing*, *supra* note 136, at 5-6 (statement of Tom Adams, Chief Executive Officer, Rosetta Stone Inc.) ("[T]he most common way for "rogue" websites . . . to reach out to American consumers is by means of paid advertisements on search engines such as Google.").

[140] S. REP. NO. 112-39, at 7 (2011) ("These parties monetize the Internet site by enabling U.S. consumers to access the infringing website, to purchase content and products off the website, and to view advertisements on the website. Without partnering with these entities, the financial incentive to run an infringing site is greatly diminished."); *IP Theft Hearing*, *supra* note 136, at 5 (statement of Tom Adams, Chief Executive Officer, Rosetta Stone Inc.) (noting that the inability of rogue websites to "utilize payment processors to transact sales with consumers will go a long way in disrupting the flow of counterfeit goods and services into the United States.").

COICA authorized the Attorney General, in actions against non-domestic domains, to serve the injunction on financial transaction providers and services that provide advertisements to Internet sites.[141] PIPA made these remedies available in actions by private rights holders, as well as in actions against domestic domains.[142] Under both COICA and PIPA, these third parties are required to implement certain "reasonable measures."[143] Financial transaction providers must ensure that their services prevent, prohibit, or suspend the completion of payment transactions between U.S. customers and sites associated with targeted domain names.[144] Additionally, COICA required financial transaction providers to provide notice to the site that it "is not authorized to use the trademark of the financial transaction provider."[145] PIPA eliminated the remedy prohibiting utilization of the financial service providers' trademarks in response to financial transaction providers' concerns about blocking use of trademarks in foreign territories.[146]

Once served with a copy of the court order/injunction, COICA required ad service providers to "take reasonable measures, as expeditiously as reasonable, to prevent its network from providing advertisements to an Internet site associated with such [nondomestic] domain name."[147] Companies who had been victimized by infringers testified that this remedy was insufficient.[148] For example, Rosetta Stone argued that ads for infringing sites should also be prohibited.[149] In response to these worries, PIPA compels ad service providers to, *inter alia*, "cease making available advertisements for that site, or paid or

---

[141] S. 3804 § 2(e)(2). In addition to serving financial transaction providers and Internet advertising services with such court orders, the Attorney General was, in actions against nondomestic domains names, also permitted to serve the orders on domain name system servers and providers of information location tools.

[142] *See* S. 968 §§ 3(d)(2)(B)&(C), 4(d)(2)(A)&(B)

[143] *See* S. 968 §§ 3(d)(2), 4(d)(2); S. 3804 § 2(e)(2)(B).

[144] *See* S. 3804 § 2(e)(2)(B)(ii)(I); S. 968, §§ 3(d)(2)(B), 4(d)(2)(A).

[145] S. 3804 § 2(e)(2)(B)(ii)(II).

[146] *IP Theft Hearing*, *supra* note 136, at 19-20 (statement of Denise Yee, Senior Trademark Counsel, Visa Inc.) ("If COICA is reintroduced . . . [a financial transaction provider] should be permitted to authorize the continued use of its trademark on foreign sites in accordance with its contractual obligations."). *Compare* S. 968 §§ 3(d)(2)(B), 4(d)(2)(A) (lacking a requirement financial transaction processors notify websites they are unauthorized to use the processors trademarked logo), *with* S. 3804 § 2(e)(2)(B)(ii)(I)-(II) (requiring trademark takedown notice by a financial transaction provider). For more information on why financial transaction providers were concerned with COICA's requirement, see the discussion of the *allofmp3.com* case in Russia, *infra* Part III.B.3.

[147] S. 3804 § 2(e)(2)(B)(iii).

[148] *IP Theft Hearing*, *supra* note 136, at 4-6 (statement of Tom Adams, Chief Executive Officer, Rosetta Stone Inc.) (arguing that restricting counterfeiters access advertising networks, payment processing and paid search engine results must be combined to effectively thwart infringement).

[149] *See id.* at 5-6 (statement of Tom Adams, Chief Executive Officer, Rosetta Stone Inc.).

sponsored search results, links or other placements that provide access to the domain name."[150]

Starving rogue websites of revenue is not a novel concept. For example, the Unlawful Internet Gambling Enforcement Act of 2006 ("UIGEA") prohibits the operators of Internet gambling websites from knowingly accepting or processing financial transactions in connection with a wager that is unlawful under a federal or state law.[151] While financial transaction providers are almost entirely immune from the statute's criminal and civil remedies,[152] they are still subject to legal obligations with respect to transactions involving unlawful Internet gambling.[153] Indeed, the financial service provider obligations contained in the law are at the core of the UIGEA's attempt to financially starve unlawful Internet gambling by cutting off its primary means of funding. These obligations require financial institutions to identify and block transactions with businesses and websites engaged in unlawful Internet gambling.[154]

---

[150] *See* S. 968 §§ 3(d)(2)(C)(ii), 4(d)(2)(B)(ii).

[151] *See* Unlawful Internet Gambling Enforcement Act of 2006, 31 U.S.C. § 5363 (2006).

[152] With respect to civil proceedings/remedies, the UIGEA broadly authorizes the Attorney General of the United States and the attorney general of any state to institute civil proceedings in any federal district court to prevent and enjoin the types of financial transactions restricted by *Id.* § 5363 (regardless of whether there has been a criminal prosecution). *Id.* § 5365(a)-(b) (2006). The law authorizes the district courts to enter temporary restraining orders, preliminary injunctions or permanent injunctions against "any person" in an effort to prevent or restrain transactions prohibited by 31 U.S.C. § 5363. *Id.* § 5365(b). Similar to the criminal provisions, there is a carve-out for financial transaction providers regarding the application of civil injunctive remedies. Specifically, § 5365(d) restricts the U.S. Attorney General and the state attorneys general from instituting civil proceedings (pursuant to 31 U.S.C. § 5365) against any financial transaction provider (assuming that the person is indeed acting as a genuine financial transaction provider). *Id.* § 5365(d). The Act also strictly limits the application § 5365 civil relief against interactive computer services "to the removal of, or disabling of access to, an online site violating section 5363, or a hypertext link to an online site violating such section, that resides on a computer server that such service controls or operates." *Id.* § 5365(c). The only scenario under which a financial transaction provider or interactive computer service could be subject to the UIGEA's criminal and/or civil remedies is where such an entity "has actual knowledge and control of bets and wagers," and operates an Internet website through which unlawful bets may be placed or received or owns or controls, or is owned or controlled by, any person who operates an Internet website where unlawful bets may be placed or received. *Id.* § 5367.

[153] The legislative history of the UIGEA states the primary reason for this back door approach, namely, that "most of the estimated 2,000 internet gambling sites today operate from offshore locations in the Caribbean and elsewhere. As such, they operate effectively beyond the reach of U.S. regulators and law enforcement as well as the statutory anti-money laundering regimes that apply to U.S.-based casinos." *See* H.R. REP. NO. 109-412, at 8-9 (2006).

[154] *See* 31 U.S.C. § 5364(a). The UIGEA mandated that the Secretary of Treasury and the Board of Governors of the Federal Reserve jointly enact regulations. 31 U.S.C. § 5364(b). These agencies adopted identical regulations. *See* 12 C.F.R. §§ 233.1-.7 (2011); 31 C.F.R.

Credit card companies can meet UIGEA's requirements by implementing a transactional coding system capable of denying authorization for transactions that have been coded as a restricted unlawful Internet gambling transaction.[155] The overriding purpose of these regulations is to require the designated payment systems (and the financial transaction provider participants within those payment systems) to establish written policies and procedures reasonably designed to identify and block, or otherwise prevent or prohibit, restricted transactions.[156] These coding mechanisms could be employed to deny transactions with websites identified as dedicated to infringing activities under the procedures outlined in PIPA.

In return for their compliance with the order and the statutory mandates, PIPA provides certain protections and immunities to any third parties required to take action under the statute. First, PIPA provides complete immunity from lawsuits and liability for any act taken by a third party that is reasonably designed to comply with the Act or reasonably arises from a court order received by the third party.[157] Second, third parties who receive such orders will not be required to take action that is not technically feasible or would cause an "unreasonable economic burden."[158] Finally, the bill encourages voluntary action by financial transaction providers and Internet advertising services and provides a safe harbor from damages in the event that such third party, in the absence of a formal court order under PIPA, voluntarily takes action already authorized by the legislation regarding an Internet site that it reasonably believes is dedicated to infringing activities.[159]

---

§§ 132.1-.7 (2010).

[155] *See* 12 C.F.R. § 233.6(d)(1)(ii); 31 U.S.C. § 132.6(d)(1)(ii). The regulations for credit card companies were "based on coding frameworks that ha[d] already been instituted by the operators of the major 'open' card systems, such as Visa, MasterCard and American Express." *See* 73 Fed. Reg. 69,382, 69,389 (Nov. 18, 2008). *IP Theft Hearing*, *supra* note 136, at 5 (statement of Denise Yee, Senior Trademark Counsel, Visa Inc.) (noting that, "In response to the [UIGEA], Visa devised a coding and blocking scheme that prevents U.S. cardholders from engaging in illegal internet gambling.").

[156] *See* 31 U.S.C. § 5364(a).

[157] *See* S. 968 §§ 3(d)(5)(A)-(B), 4(d)(5)(A)-(B).

[158] *See id.* §§ 3(e)(3), 4(e)(3). Assertions of technical feasibility or economic hardship would, under the terms of the bill, need to be asserted as an affirmative defense to a separate action authorized by § 3(e)(1) and § 4(e)(1) to compel compliance from third parties that have knowingly and willfully failed to comply with court orders they have received. *Id.* §§ 3(e)(1), 4(e)(1).

[159] *See id.* § 5(a). *See also IP Theft Hearing*, *supra* note 136, at 5 (statement of Denise Yee, Senior Trademark Counsel, Visa Inc.) (noting other areas where Visa works cooperatively with the private sector and law enforcement agencies to combat other forms of illegal activity that online merchants engage in such as child pornography, identity theft, data breaches, illegal tobacco sales, and counterfeit pharmaceutical sales); *DPE Commends Agreements to Curb Digital Theft, Notes Government Leadership*, THE DEPARTMENT FOR PROFESSIONAL EMPLOYEES (AFL-CIO) (July 12, 2011), *http://commcns.org/sRBWyM*

3. Recourse Against Domain Names and Service Providers

Actions brought pursuant to Operation in Our Sites are limited to Internet sites with a U.S.-based registry.[160] This limitation is problematic because many rogue websites are not domestic.[161] COICA targeted this issue by authorizing the AG to bring *in rem* actions for injunctions against domain names used by sites dedicated to infringing activities that had a domestic or non-domestic registry or registrar.[162] If the domain name had a non-domestic registry or registrar, the statute permitted an *in rem* action if those sites were dedicated to infringing activity, conducted business directed at U.S. residents, and harmed holders of U.S. intellectual property rights.[163] As with current law, this action would have only been against the domain name and not the site. The injunctions permitted under COICA could be served on non-related entities involved in the domain name system: the registry/registrar of domestic domains, who would have to suspend operation of and lock the domain name, and service providers for non-domestic domains, who would have to block the domain name from resolving to the IP address.[164]

PIPA made a number of changes to COICA to ensure that third parties who may be required to take action as result of a court order receive notice and an opportunity to participate in the proceeding.[165] As with COICA, although with additional due process protections, orders granted in actions brought by the AG against nondomestic domain names may be served on operators of non-authoritative domain name system servers[166] (presumably, ISPs) and

---

(documenting where different payment system operators voluntarily agreed to maintain procedures to suspend or terminate payment services to merchants that intentionally and systematically infringing products over the Internet); Greg Sandoval, *MasterCard Willing to Cut Off Pirate Sites*, CNET NEWS (Dec. 16, 2010), http://commcns.org/rRAZMT.

[160] *See* discussion, *supra* Part II.B.1.

[161] *See* S. REP. NO. 112-39, at 3-4 (2011).

[162] S. 3804 § 2(c).

[163] *Id.* § 2(d)(2)(A).

[164] *Id.* § (2)(e)(1)-(2). The definition of service provider in COICA borrows from the very broad definition in 17 U.S.C. § 512(k)(1). It includes 17 U.S.C. § 512(k)(1)(A) (defining a "service provider" as "an entity offering the transmission, routing, or providing of connections for digital online communications, between or among points specified by a user, of material of the user's choosing, without modification to the content of the material as sent or received") as well as 17 U.S.C. § 512(k)(1)(B) (defining a "service provider" as "a provider of online services or network access, or the operator of facilities therefor, and includes an entity described in subparagraph (A)"). As a result, information location tools are included under this definition.

[165] *See* discussion, *infra* Part III.B.2.

[166] Non-authoritative name servers do not contain copies of any domains. Instead they have a cache file that is constructed from all the DNS lookups it has performed in the past for which it has gotten an authoritative response. When a non-authoritative server queries an authoritative server and receives an authoritative answer, it passes that answer along to the querier as an authoritative answer. Thus, non-authoritative servers can answer

information location tools.[167] Unlike COICA, PIPA does not authorize recourse against registries and only permits recourse via non-authoritative domain name servers or information location tools in AG actions against non-domestic domain names.[168]

When served with an injunction against a site dedicated to infringing activity, non-authoritative domain name system servers must take the "least burdensome technically feasible and reasonable measures" to prevent the domain name from resolving to the IP address.[169] Information location tools must remove or disable access to the Internet site associated with the domain name, rather than the domain name itself, which might include parallel sites as well.[170] Information location tool providers also must refrain from providing hyperlinks to the infringing site.[171] These remedies are unavailable to private rights holders and in AG actions against domestic domains.[172] Presumably, the AG would use the current law to proceed against domestic domain names in order to block the domain names.[173]

PIPA provides immunity from lawsuits and liability for any act by a non-authoritative domain name system server or provider of information location tools that is reasonably designed to comply with the Act or reasonably arises from a court order.[174] Third parties who receive such orders will not be required to take action that is not technically feasible or that would cause an economic burden.[175] However, PIPA does not provide a safe harbor for damages arising from voluntary actions taken by non-authoritative domain name system servers and information location tools providers, as it does for advertising services and financial transaction providers.[176]

---

authoritatively for a given resolution request. However, non-authoritative servers are not authoritative for any domain they do not contain specific zone files for. Most often, a non-authoritative server answers with a previous lookup from its lookup cache. Any answer retrieved from the cache of any server is deemed non-authoritative because it did not come from an authoritative server. *See Non-Authoritative DNS Servers*, http://commons.org/vBi0oa.

[167] S. 968 § 3(d)(2).

[168] *Compare* S. 3804 § 2(c), *with* S. 968 § 3(c)(1)(B).

[169] S. 968 § 3(d)(2)(A)(i).

[170] *Id.* § 3(d)(2)(D)(i).

[171] *Id.* § 3(d)(2)(D)(ii).

[172] *Id.* § 3(a) (noting that the Attorney General can commence action against non-domestic domains).

[173] *See* discussion, *supra* Part II.B.

[174] *Id.* § 3(d)(5)(B).

[175] *Id.* §§ 3(d)(2), 4(d)(2).

[176] *See id.* § 5(a). However, Section 5 of PIPA protects these parties from liability if they voluntarily stop providing or refuse to provide services to sites that endanger the public health by selling or distributing prescription medication or adulterated or misbranded medication or selling/distributing medication. *Id.* § 5(b).

4. Private Rights of Action

PIPA authorizes a private rights holder who is the victim of infringement to bring an action against a domain name or the owner or registrant of an Internet site dedicated to infringing activity.[177] Specifically, Section 4 of PIPA enables private rights holders and the AG to bring actions against both domestic and foreign domain names.[178]

During Congressional hearings discussing COICA, rights holders argued that it would be unrealistic to expect the DOJ to increase enforcement significantly in a period of budget deficits and, therefore, urged Congress to include a private right of action in the legislation.[179] In essence, these rights holders argued that they should not be forced to rely on the government and should be able to seek recourse themselves.

Other parties expressed concern about private actions. Testifying before the Senate Judiciary Committee, representatives from Verizon noted that "private plaintiffs, unlike the DOJ, are acting in their own interests and are far less likely to weigh the costs that their enforcement requests impose on third parties and, more broadly, U.S. national interests in promoting a global Internet."[180] As a result, private actions would result in "over-broad implementation of domain name restrictions."[181] Similarly, Google argued that including a private right of action in any legislation "would invite suits by 'trolls' to extort settlements from intermediaries or sites who are making good faith efforts to comply with the law."[182]

PIPA has attempted to incorporate these concerns. While Section 4 of the bill provides for a private right of action against the registrant of the domain name or the owner or operator of an Internet site dedicated to infringing activity, its remedies are limited compared to the Section 3 remedies available to the AG against nondomestic domains.[183] For instance, a court order issued

---

[177] *Compare* S. 968 §§ 2(11)(b), 4(a)(1)(A), *with* S. 3804 § 2(b)-(c) (naming the Attorney General as the only party enabled to seek injunctive relief or commence an *in rem* action against a site dedicated to infringing activities).

[178] Although the Senate has noted that PIPA does not authorize the Attorney General to bring an action against U.S.-registered domains, Section 4 of the legislation does authorize the Attorney General to bring such suits. S. 968 § 4(a)(1)-(2). A "qualifying plaintiff," defined to include the Attorney General, may bring an action under Section 4. *Id.* § 2(11).

[179] *IP Theft Hearing*, *supra* note 136, at 6-7 (statement of Tom Adams, CEO, Rosetta Stone Inc.).

[180] *Id.* at 6.

[181] *Id.*

[182] *Online Commerce Hearing I*, *supra* note 60, at 7 (statement of Kent Walker, Senior Vice President and General Counsel, Google Inc.).

[183] S. 968 §§ 3-4 (Section 3 authorizes Attorney General action against foreign rogue websites, while Section 4 authorizes private rights holders and Attorney General actions against foreign and domestic domains).

in a private right of action that complies with the requisite notice procedures can only be served on financial transaction providers and Internet advertising agencies.[184] While PIPA does not enable a private rights holder to serve a court order on third party domain name system servers or information location tools, it nonetheless gives private rights holders a wide panoply of enforcement tools, especially in conjunction with other remedies.[185]

B. Concerns with Recent Legislative Proposals

1. First Amendment Issues

Critics of COICA and PIPA raise First Amendment concerns akin to those raised against Operation In Our Sites.[186] For example, EFF argues that "requiring search engines to remove links to an entire website raises serious First Amendment concerns considering the lawful expression that may be hosted on the same domain."[187] Critics believe that allowing authorities to shut down entire domains, rather than only the allegedly infringing part of a website, will effectively censor "vast amounts of legitimate, protected speech" and that "by allowing this censorship of the internet the United States will join the ranks of the non-democratic, totalitarian regimes of the world that already engage in the practice."[188]

Recently, a group of law professors submitted a joint statement to members of Congress urging them to reject PIPA.[189] In the letter, they note that PIPA:

> authorizes courts to take websites "out of circulation"—to make them unreachable by and invisible to Internet users in the United States and abroad—immediately upon application by the Attorney General after an *ex parte* hearing. No provision is made for any review of a judge's *ex parte* determination, let alone for a "prompt and final judicial determination, after an adversary proceeding," that the website in question contains unlawful material.[190]

Due to the lack of protections, the professors argue that PIPA falls short of the Constitution's requirements for eliminating speech from public circulation.[191]

---

[184] *Id.* § 4(d).

[185] *See* discussion, *supra* Part II.A.

[186] *See* discussion, *supra* Part II.B.3.

[187] Abigail Phillips, *The "PROTECT IP" Act: COICA Redux*, ELECTRONIC FRONTIER FOUNDATION (May 12, 2011), http://commcns.org/sBjhlk.

[188] *Proposed Bill Attempts to Take the Wind Out of the Sails of Internet Piracy*, MICH. TELECOMM. & TECH. L. REV. BLOG (Sept. 27, 2010), http://commcns.org/scjJZ8.

[189] John Allison et al., Professors' Letter in Opposition to "Preventing Real Online Threats to Economic Creativity and Theft of Intellectual Property Act of 2011" (PROTECT-IP Act of 2011, S. 968) (July 5, 2011), http://commcns.org/uKLHkb.

[190] *Id.* at 3.

[191] *Id.*

Supporters of the legislation counter that the bills are not constitutionally overbroad. First Amendment expert Floyd Abrams claimed that the procedural protections "are so strong, uniform and constitutionally rooted that it is no exaggeration to observe that any complaints in this area are not really with the bill[s], but with the Federal Rules of Civil Procedure itself."[192] Instead, Abrams argues, COICA and PIPA focus "on a narrow category of entities which are not simply trafficking in some infringing content, or occasionally breaking federal laws, but which are primarily [and continuously] devoted to providing or selling infringing content in the United States."[193] While accepting that some non-infringing or otherwise protected content may be blocked as a result of a blocked domain name, Abrams posits that the proposed bills are "sufficiently narrow to accommodate the immediate publication of that content elsewhere and the future publication of the content on the same domain."[194] Additionally, he points out that under current case law, the "presence of non-infringing speech generally does not provide a copyright violator with immunity from enforcement actions."[195]

Other supporters point out that the proposed legislation "provides that a domain name may only be blocked after an *in rem* proceeding is commenced and a court issues an injunction — preliminary or otherwise. As such, under current law, COICA's provisions are no more a prior restraint than the preliminary injunctions routinely ordered in infringement cases."[196] As a result, it would be foolish to think that no case could result in a substantial amount of protected speech being blocked.[197] Nonetheless, the possibility of a violation of a particular defendant's First Amendment rights does not mean that the bills are unconstitutional on their face.[198]

---

[192] Letter from Floyd Abrams, Partner, Cahill Gordon & Reindel LLP, to Patrick Leahy, Chairman, S. Comm. on the Judiciary, et al., at 8 (Feb. 11, 2011), *available at* http://commcns.org/tefmoD [hereinafter Abrams COICA Letter]; Letter from Floyd Abrams, Partner, Cahill Gordon & Reindel LLP, to Patrick Leahy, Chairman, S. Comm. on the Judiciary, et al., at 10 (May 24, 2011), *available at* http://commcns.org/uJSNLw [hereinafter Abrams PIPA Letter].

[193] Abrams COICA Letter, *supra* note 192, at 6; Abrams PIPA Letter, *supra* note 192, at 8.

[194] Abrams COICA Letter, *supra* note 192, at 7; Abrams PIPA Letter, *supra* note 192, at 8-9.

[195] Abrams COICA Letter, *supra* note 192, at 7; Abrams PIPA Letter, *supra* note 192, at 8.

[196] Terry Hart, *COICA: First Amendment*, COPYHYPE (Nov. 29, 2010), http://commcns.org/sIfP8d.

[197] *Id.*

[198] *Id.*

2. Due Process Concerns

Both COICA and PIPA offer greater due process protections than the current law used against the domestic domain names in Operation in Our Sites. While Operation In Our Sites relies on civil seizure and forfeiture,[199] COICA and PIPA provide for equitable remedies and do not create any causes of action for seizure or forfeiture.[200] In other words, the domain name is merely blocked, not forfeited, and the owner of the domain name can move to modify, vacate or suspend the order when it ceases any infringing activities.

Under COICA and PIPA, and in accordance with Rule 65 of the Federal Rules of Civil Procedure, a court may issue a temporary restraining order, preliminary injunction or an injunction against a domain name, registrant of a domain name, or owner/operator of a website to cease and desist from undertaking any further infringing activities.[201] Remedies under Rule 65 require notice and a much higher threshold than the probable cause needed to seize domain names under Operation in Our Sites.[202] In doing so, both bills offer "the procedural protections that federal law currently affords all litigants in civil actions in the United States."[203]

To obtain a permanent injunction, the government must show: (1) irreparable injury; (2) that remedies available at law are inadequate to compensate for that injury; (3) that the balance of hardships between the plaintiff and defendant warrants a remedy in equity; and (4) that the public interest would not be disserved by a permanent injunction.[204] For preliminary injunctions, the government also would need to show either a likelihood of success on the merits or sufficiently serious questions to make them a fair ground for litigation, as well as a balance of hardships "tipping decidedly" in its favor.[205] As a result, the AG would need to demonstrate a likelihood of success on the merits rather than simply establishing probable cause.[206]

Rule 65 also provides that a preliminary injunction may issue "only on notice to the adverse party."[207] For a temporary restraining order to issue without notice, two conditions must be satisfied. First, the facts contained in an affidavit or a complaint must "clearly show that immediate and irreparable

---

[199] *See* discussion, *supra* Part II.B.2.

[200] S. 968 §§ 3(e)(1)-(2), 4(e)(1)-(2); S. 3804 § 2(g)(1)-(2).

[201] S. 968 § 3(b)(1).

[202] *Id.* §§ 3(b)(1); S. 3804 § 2(b).

[203] Abrams COICA Letter, *supra* note 192, at 5; Abrams PIPA Letter, *supra* note 192, at 5.

[204] *See, e.g.*, Ebay Inc. v. MercExchange, L.L.C., 547 U.S. 388, 391 (2006).

[205] *See* Salinger v. Colting, 607 F.3d 68, 75 (2nd Cir. 2010). *See also* Perfect 10, Inc. v. Google, Inc. 653 F.3d 976 (9th Cir. 2011).

[206] *See* Salinger, 607 F.3d at 79, 80.

[207] Fed. R. Civ. P. 65(a)(1).

injury, loss, or damage will result to the movant before the adverse party can be heard in opposition."[208] Second, the attorney for the plaintiff must certify, "in writing, any efforts that have been made to give notice, as well as the reasons why notice should not be required."[209]

Unlike the ex parte procedures used in Operation In Our Sites, COICA required that, simultaneously to bringing an *in rem* action against a domain name, the AG must serve the registrant with notice of the alleged violation and the intent to proceed under COICA and must publish notice of the action promptly after filing.[210] COICA also permitted any party required to take action based on a COICA order to petition the court to modify, suspend, or vacate it based on evidence that the site associated with the domain name is no longer participating in, or never was, dedicated to infringing activity, or if the interests of justice so require.[211]

Even with the numerous notice provisions outlined above, critics of COICA argued that the bill provided operators of websites dedicated to infringing activity more procedural protections than other parties who also might be involved.[212] For instance, while the DOJ could impose obligations by serving orders on domain name system servers, financial transaction providers, and advertising networks, COICA did not allow these innocent third parties to first have an opportunity to be heard in court, as it did for the operators of targeted websites.[213]

Heeding these concerns, Congress provided additional due process protections in PIPA. Under the proposed bill, the AG first must attempt to bring an *in personam* action; only if he or she is unable to locate the registrant, owner, or operator, or if no such person has a U.S. address, may the Attorney General bring an *in rem* action.[214] This provision provides a higher level of protection by enabling the site's owner or registrar to appear to defend the action, if he or she can be located.[215] PIPA also contains notice requirements designed to protect innocent third party service providers. Any third party that may be required to take action if the court issues an order must be identified in the suit and provided notice when the suit commences.[216] Identified third parties may intervene at any time and may subsequently seek an order to

---

[208] Fed. R. Civ. P. 65(b)(1)(A).
[209] Fed. R. Civ. P. 65(b)(1)(B).
[210] S. 3804 § 2(c)(1)(B).
[211] *Id.* § 2(h)(2).
[212] *See* Letter from Markham C. Erickson, Exec. Director, NetCoalition, to Patrick Leahy, Chairman, S. Comm. on the Judiciary, at 2 (Nov. 15, 2010) [hereinafter *EFF COICA Letter*], *available at* http://commcns.org/shj6Gg.
[213] *See id.*
[214] S. 968 § 3(a)(2).
[215] *Id.* § 3(c)(a).
[216] *Id.*

modify, suspend, or terminate an order.[217] Additionally, court approval must be obtained before an order may be served on an operator of a non-authoritative domain name system, a financial transaction provider, an Internet advertising service. or an information location tools provider.[218]

The ability of the AG to use different laws to block access to domestic and non-domestic domain names will create a situation where foreign domain names have more due process than domestic names. For instance, the AG would use the current law, which permits *ex parte* seizure on a showing of probable cause, to block a domestic domain name, but would need to use PIPA, which provides more due process to the domain name and affected third parties, to compel Internet service providers and information location tools to block a non-domestic domain name.

3. *Extraterritoriality*

COICA contained remedies that had a potential extraterritorial impact. While financial transaction providers only needed to block transactions from customers located in the U.S., the bill failed to place geographic limits on the obligation of financial transaction providers to block use of their trademark or the obligations of ad service providers and Internet service providers.

The law's expansive reach did not go unnoticed, and concerns about COICA's extraterritorial impact were raised. In a November 2010 letter to Senator Leahy, the NetCoalition noted that,

> In addition to authorizing U.S. courts to exercise jurisdiction over foreign activity, COICA creates extraterritorial remedies. A financial transaction provider would be required to prevent the use of its trademarks on foreign websites. Similarly, an advertising network would be required to stop placing contextual or display ads on foreign websites. This would be the case even if a U.S. user no longer can access the site or purchase infringing material from it. Once again, this could be a dangerous precedent that could be exploited by other countries against U.S. businesses.[219]

Visa worried that such a requirement would put financial transaction providers in jeopardy of violating other countries' laws.[220] For instance, it explained that in 2006, it received a documented complaint by copyright owners that the Russian website AllofMP3.com was infringing their copyrights.[221] After an investigation, Visa concluded that under Russian law, as well as the laws of the majority of Visa's customers, the merchant's transactions were illegal.[222] In

---

[217] *Id.* §§ 3(f)(4), 4(f)(4).
[218] *Id.* §§ 3(d)(1)-(2), 4(d)(1)-(2).
[219] EFF COICA Letter, *supra* note 212, at 2.
[220] *See IP Theft Hearing*, *supra* note 136, at 8-9 (statement of Denise Yee, Senior Trademark Counsel, Visa, Inc.).
[221] *See id.* at 7-9.
[222] *See id.*

response, and after appropriate notice, Visa's Russian affiliate bank stopped processing Visa transactions for the website.[223] Visa was then sued by AllofMP3.com in Russia.[224] Finding in favor of the website, a Russian court concluded that the bank violated its contract with the merchant and ordered it and Visa to continue providing processing services.[225] Although COICA would not require Visa to block foreign transactions, a refusal to permit use of its trademark might have also run afoul of Russian law.

Verizon and Visa suggested modifications to the bill to help alleviate extraterritorial problems. Visa suggested that a financial transaction provider should be permitted to authorize the continued use of its trademark on foreign sites in accordance with its contractual obligations.[226] Similarly, Verizon recommended modifications to clarify that judicial orders apply only to service providers' DNS servers located within the United States. In doing so, Verizon noted that a judicial order requiring a service provider to "restrict access to domain names on international servers . . . not only increases the burden on and cost for service providers, it may create an extraterritorial impact that could open the legislation to legal challenge in foreign courts against which the bill does not and cannot provide immunity."[227]

As to COICA's requirement that service providers block the domain name from resolving to the IP address, if limited to Internet access providers, there would have been an inherent geographic limitation because these providers only provide access in a specific location. However, the definition of service provider in COICA was not limited to the access providers, but also included information location tools, such as search services like Google.[228] Under COICA, therefore, information location tools like Google presumably would have been required to provide dead links or block access to its cache of the infringing domain name's website. Moreover, since there was no geographical limitation on recourse required by the service provider, Google may have been obligated to serve up dead or no links in China and Russia.

While PIPA added remedies against financial transaction providers and Internet advertising services in actions against domestic domain names, the Senate made a number of changes to the bill to minimize the extraterritorial concerns. First, the remedies available to the AG against operators of non-

---

[223] *See id.*

[224] *See id.*

[225] *See id.*

[226] *See IP Theft Hearing*, *supra* note 136, at 19 (statement of Denise Yee, Senior Trademark Counsel, Visa, Inc.).

[227] *See id.* at 4 (statement of Thomas M. Dailey, Vice President and Deputy General Counsel, Verizon Commc'ns Inc.).

[228] S. 3804 §§ (2)(e)(1)-(2). *See* discussion, *supra* note 164 (definition of service provider).

authoritative domain name system servers have been geographically limited, meaning operators are not required to take any measures on domain name system servers located outside the U.S.[229] Additionally, financial transaction providers are no longer obligated to stop use of their trademarks on infringing sites. Interestingly, PIPA completely eliminated remedies prohibiting utilization of the financial service provider trademark, even in the U.S., instead of prohibiting only the domestic use of the trademark.

However, PIPA does maintain some remedies that might have extraterritorial reach. For instance, in an action against a non-domestic domain brought by the AG, operators of non-authoritative domain name system servers must prevent the domain name from resolving to the IP address in foreign countries if the domain name system server is located in the U.S.[230] Similarly, in such actions, information location tool providers are required to disable access and hyperlinks to the site associated with the domain name not only within the U.S., but also in foreign countries.[231] Finally, ad service providers must prohibit ads appearing on or for the site in foreign countries as well as in the U.S. [232]

Even assuming that a law is presumed not to be extraterritorial, PIPA is designed to reach non-domestic domains. Of its four possible remedies—blocking financial transactions of *U.S. customers*, blocking *U.S.-based* non-authoritative domain name system servers from resolving to the domain's IP address, not providing advertisements, and requiring information location tools to block access to the site associated with the non-domestic domain name—two contain explicit geographical limitations, implying that the other remedies do not have such limitations.[233] The presumption against extraterritoriality, therefore, may not be sufficient to limit the possible extraterritorial interpretation of the non-limited remedies contained COICA or PIPA.

Many have also raised concerns about the potential consequences of the extraterritorial application of U.S. copyright law.[234] For example, VISA notes that "[t]he extraterritorial application of U.S. law may invite retaliation by other countries' governments."[235] As the company explains,

---

[229] S. 968 § 3(d)(2)(A)(i).

[230] *Id.*

[231] S. 968 § 3(d)(2)(D).

[232] See EFF COICA Letter, *supra* note 212, at 2.

[233] S. 968 § 3(d)(2).

[234] *See, e.g.*, *IP Theft Hearing*, *supra* note 136, at 16-17 (statement of Denise Yee, Senior Trademark Counsel, Visa Inc.). *See also* Letter from Gregory A. Jackson, Vice President for Policy and Analysis, Educause, to Patrick J. Leahy, Chairman, S. Comm. on the Judiciary, at 3 (Sept. 27, 2010), *available at* http://commcns.org/uHuhsC; *EFF COICA Letter*, *supra* note 212, at 2 (arguing that "this approach could set a dangerous precedent for foreign countries to attempt to control content on U.S. websites.").

[235] *IP Theft Hearing*, *supra* note 136, at 16 (statement of Denise Yee, Senior Trademark

> European countries, for example, believe that many U.S. companies infringe European laws concerning geographical indicators. Under European law, only wineries in the Champagne region of France can call sparkling wine "champagne," and only cheese manufacturers in the Parma region of Italy can use the name "parmesan cheese." European countries could require payment systems [or search engines] to stop processing transactions for [or linking to] U.S. merchant websites that sell products that violate European laws concerning geographical indicators. Similarly, repressive governments could force payment systems to stop doing business with legitimate U.S. merchants that sell books critical of their regimes to residents of their countries.[236]

Although PIPA addressed many of the concerns about extraterritoriality, to clarify remaining concerns, it could explicitly limit the other two remedies geographically as well: "reasonable measures to prevent advertising networks from providing advertisements *on foreign sites' website displays in the U.S.* and to cease making available advertisements for the site, or paid or sponsored search results, links or other placements that provide access to the domain name *in the U.S.*"[237] and "reasonable measures by information location tools to remove or disable access to the Internet site *in the U.S.* and to not serve up a hypertext link to such site *in the U.S.*"[238]

Some argue that certain countries may rely on this law as precedent to justify retaliation against U.S. websites. NetCoalition argued that "this approach could set a dangerous precedent for foreign countries to attempt to control content on U.S. websites."[239] It pointed to examples where "a French court found Yahoo liable for hosting auctions of Nazi paraphernalia that were viewable in France" and where "an Australian court exercised jurisdiction over Barron's for alleged defamation in an article posted on a U.S. website."[240] In a more extreme example, Visa noted "repressive governments could force payment systems to stop doing business with legitimate U.S. merchants that sell books critical of their regimes to residents of their countries."[241] Of course, limiting the potential extra-territorial remedies, as discussed above, would help ameliorate these concerns.

Counsel, Visa Inc.).

[236] *IP Theft Hearing*, *supra* note 136, at 17 (statement of Denise Yee, Senior Trademark Counsel, Visa Inc.). Although the actual quote here addressed payment processor issues, the payment processor language was modified to address this issue in PIPA, but the same issue with respect to search engines has not been addressed.

[237] The italicized text is the authors' suggested additions.

[238] S. 968 § 3(d)(2)(C).

[239] EFF COICA Letter, *supra* note 212, at 2.

[240] *Id.*

[241] *IP Theft Hearing*, *supra* note 136, at 17 (testimony of Denise Yee, Senior Trademark Counsel, Visa Inc.).

4. Internet Security

As discussed, PIPA would deny users access to illegal sites in a slightly different way than Operation In Our Sites. The proposed legislation authorizes the AG to obtain an order that requires an operator of a non-authoritative domain name server, including ISPs, "to prevent the domain name described in the order from resolving to that domain name's Internet protocol address."[242] This process often is referred to as Domain Name System (DNS) filtering.[243]

Essentially, DNS filtering prevents DNS inquiries for a particular domain names from reaching the root servers for those names.[244] Because DNS filtering occurs at the ISP level, only customers of ISPs that have been ordered to filter are denied access to the site; as a result, the site is still accessible from outside the U.S.[245] Advocating instead for DNS blocking in her testimony before the House Subcommittee on Intellectual Property and the Internet, GoDaddy's Executive Vice-President and General Counsel, Christine N. Jones explained the difference, noting that "DNS blocking provides a much more thorough solution [than DNS filtering] because it applies to all Internet users, regardless of which ISP they are a customer of or whether proxy servers are used."[246] While DNS blocking is currently employed in Operation In Our Sites and is effective against sites that register their domain names with U.S.-based registrars (.com or .net)—over which U.S. law enforcement already has jurisdiction—law enforcement lacks the jurisdiction to apply DNS blocking to prevent sites owned, operated, and registered overseas from offering pirated and counterfeit goods to U.S. consumers. For that reason alone, DNS blocking cannot be the solution for tackling illegal foreign sites.

Opponents of DNS filtering note that Internet security remains a top priority of the Obama Administration.[247] To improve this security, they argue, the Federal Government must continue to promote the adoption of a new security protocol, commonly referred to as Domain Name System Security Extensions (DNSSEC).[248] Generally, the protocol requires that any response to a request

---

[242] S. 968 § 3(d)(2)(A)(i).

[243] *See Internet Society Perspectives on Domain Name System (DNS) Filtering*, INTERNET SOCIETY, http://commcns.org/tn0KS1 (last visited Dec. 15, 2011).

[244] *Online Commerce Hearing II*, *supra* note 67, at 9 (statement of Christine N. Jones, Executive Vice-President, General Counsel, & Corporate Secretary, The Go Daddy Group, Inc.).

[245] *Id.* at 10.

[246] *Id.* at 9.

[247] *See* CROCKER ET AL., SECURITY AND OTHER TECHNICAL CONCERNS RAISED BY THE DNS FILTERING REQUIREMENTS IN THE PROTECT IP BILL 5 (2011), http://commcns.org/syU0Br (in addition to being DNS experts, many of the authors are also senior officials with ICANN, founders of their own Internet security companies, or advisors to leading Internet companies on Internet security).

[248] *See id.* at 5-6.

from a particular site would include a verification that the site, and not a third party, responded to the request.[249] DNSSEC's main objective is to protect consumers and sites from attacks in which an attacker intercepts a digital conversation and steals the victim's security data by pretending to be a trusted source.[250]

Some concerns about DNS filtering are based on allegations that it will interfere with DNSSEC. Specifically, opponents contend that "[r]eplacing responses with pointers to other sources, as [PIPA] would require, is fundamentally incompatible with end-to-end DNSSEC" because DNSSEC compliant software would not accept a response that did not include the necessary verification.[251] Critics of this concern argue that DNS filtering does not endanger DNSSEC because its effect will be extremely limited; only websites listed on the court order will be blocked, leaving all other sites and their DNS data completely unaffected.[252] They also note that any blocking implemented via the proposed legislation would be entirely consistent with law enforcement efforts to block other illegal activities, including the distribution of child pornography over the Internet.[253]

Many also worry that DNS filtering risks causing collateral damage if not implemented properly, including the inadvertent take down of legitimate sites.[254] They point to ICE's seizure of the website mooo.com that targeted 10 websites that provided explicit child pornographic content, but also led to the wrongful takedown of over 84,000 subdomains.[255] These fears, however, neglect the fact that PIPA includes a host of procedural safeguards designed to protect legitimate sites, as well requiring the AG to show that a targeted site is dedicated to infringement, making such collateral damage highly unlikely.[256] Moreover, ISPs already filter IP addresses to combat spammers, phishers, and

---

[249] *See id.* at 6.

[250] *See* Matthew Lasar, *DNS Filtering: Absolutely the Wrong Way to Defend Copyrights*, ARS TECHNICA (May 27, 2011), http://commcns.org/sPBWYZ.

[251] CROCKER, *supra* note 247, at 6.

[252] *See* George Ou, *DNS Filtering is Essential to the Internet*, HIGH TECH FORUM 6 (2011), http://commcns.org/tBK8VG.

[253] *See id.* at 5.

[254] *See id.* at 4.

[255] *See* Thomas Claburn, *ICE Confirms Inadvertent Web Site Seizures*, INFORMATIONWEEK (Feb. 18, 2011), http://commcns.org/ufeCLe. *See also* Press Release, Joint DHS-DOJ "Operation Protect Our Children" Seizes Website Domains Involved in Advertising and Distributing Child Pornography, DEP'T OF HOMELAND SEC. (Feb. 15, 2011), http://commcns.org/tHflEY.

[256] *See* Press Release, Sen. Patrick Leahy, Leahy, Hatch, Grassley Unveil Targeted Bill To Counter Online Infringement (May 12, 2011), http://commcns.org/ux8GBg (stating that legislation was written to limit law enforcement authority to go after "the 'worst-of-the-worst' websites dedicated to selling infringing goods").

other commercially motivated undesirable conduct.[257]

There may also be a solution so that both the filtering called for in the legislation and DNSSEC can coexist without modification. Instead of redirecting users, DNSSEC may be designed to handle an error message sent from the user's ISP indicating that the site is blocked, similar to other error messages currently sent by ISPs when a site is busy or down.[258] Detractors of this compromise argue that DNSSEC compliant software could not accept an error message instead of a verified response from the site because users "have a need to distinguish between policy-based failures and failures caused [by hackers]."[259]

Critics of the bill argue that customers of ISPs ordered to block sites will stop using the ISPs' DNS server, and will switch to DNS servers that do not filter, including those located overseas.[260] By turning to rogue DNS servers located overseas, they contend, users expose their financial and other personal information to theft from the same types of criminals running pirate sites.[261] They further argue that the filtering provisions of the bill will be ineffective because of the number of circumvention tools that have been developed, including the Firefox browser plug-in offered by MAFIAAFire, to automatically redirect users to a seized domain name using the domain name's IP address.[262]

Because alternate DNS servers exist, it stands to reason that some users have already made the switch and will continue to use alternate DNS servers.[263] Even before users worried that law enforcement might block their access to their favorite illegal sites, sophisticated users began switching to alternative DNS servicers for other reasons, including improving access speed and preventing phishing websites from loading on their computers.[264] Thousands of private open DNS systems already exist, with no indication thus far that using such alternate DNS poses additional threats.[265] However, most consumers will

---

[257] *See* Ou, *supra* note 252, at 4 (noting that author Paul Vixie was instrumental in the development of this type of blocking technology).

[258] *See DNSSEC Validation Failure FAQs*, COMCAST, http://commcns.org/sUxWIu (last visited Dec. 15, 2011) (explaining that the DNS will send an error message to the requesting computer which will be displayed by its browser).

[259] *See* CROCKER, *supra* note 247, at 6.

[260] *Id.* at 9.

[261] *See id.*

[262] *See id.*

[263] *See id.* 9-10 (stating that by turning to rogue DNS servers located overseas, these users expose their financial and other personal information to theft from the same types of criminals running pirate sites).

[264] *See* Amit Agarwal, *OpenDNS – What is OpenDNS and Why You Absolutely Need It?*, DIGITAL INSPIRATION (Mar. 16, 2008), http://commcns.org/ufGaZe.

[265] *See* Ou, *supra* note 252, at 7.

not go through the process of switching DNS providers or installing a plug-in just to access pirate or counterfeit sites.[266] While some users may find it easy to get around DNS filtering, arguably the bill achieves its purpose if it cuts off these sites from the vast majority of U.S. consumers, making the Internet a more "habitable environment."[267]

Despite the criticism, denying access to illegal sites has yielded significant positive results. Blocked sites often must move to new domain names, causing them to lose the Internet ratings history they had acquired and hugely impacting both advertising revenues and search result rankings.[268] John Morton, the Director of Immigration and Customs Enforcement (ICE), pointed out that ICE's first action to take down illegal sites led many other sites that offer pirated content and counterfeit products to voluntarily shut down.[269] Commenting on the Operation in Our Sites' takedowns, he noted that he had "never seen that kind of deterrence come from a single law enforcement action" in all his years in law enforcement.[270] Moreover, as Attorney General Eric Holder noted, site takedowns serve to educate consumers of the risks posed by illegal sites.[271]

While both sides of the issue make legitimate arguments for why blocking access to websites may or may not conflict with Internet security protocols, both sides lack reliable evidence to support their positions. U.S. consumers and businesses should be able to use the Internet safely as their preferred vehicle for conducting legitimate business, which includes being protected from both counterfeiters/infringers and hackers.

---

[266] *See* Press Release, Sen. Patrick Leahy, Senators Introduce Bipartisan Bill To Combat Online Infringement (Sept. 20, 2010), http://commcns.org/uiYBgW ("American consumers are too often deceived into thinking the products they are purchasing at these websites are legitimate because they are easily accessed through their home's Internet service provider, found through well-known search engines, and are complete with corporate advertising, credit card acceptance, and advertising links that make them appear legitimate."). *See also* Press Release, Dep't of Justice, Attorney General Eric Holder Speaks at the Operation in Our Sites II Press Conference (Nov. 29, 2010) [hereinafter Holder Press Release], http://commcns.org/t6t8mh ("With today's seizures, we are disrupting the sale of thousands of counterfeit items. We are cutting off funds to those looking to profit from the sale of illegal goods and exploit the ingenuity of others. And, as the holiday shopping season gets underway, we are also reminding consumers to exercise caution when looking for deals and discounts online.").

[267] *See* Ou, *supra* note 252, at 4.

[268] *See Alexa Internet – Company Overview*, ALEXA (Sept. 30, 2011), http://commcns.org/srOfz1. *See also How are Alexa's Traffic Rankings Determined?*, ALEXA (Sept. 30, 2011), http://commcns.org/uN5JzB.

[269] *See* Juliana Gruenwald, *Customs Chief Defends Seizure Of Domain Names*, NAT'L J. (Jan. 18, 2011), http://commcns.org/sJav8D.

[270] *Id.*

[271] Holder Press Release, *supra* note 266.

IV. CONCLUSION

The Internet is a powerful platform for the production and distribution of creative works, providing benefits for authors, copyright owners, users, and the public at large. But realizing the Internet's great potential will require meeting the serious and growing problem of online piracy and counterfeiting. Protecting intellectual property in the digital environment is essential to our nation's economic growth, to maintaining and creating jobs, to protecting consumers, and to the competitiveness of American businesses in markets throughout the world. The Federal Communications Commission recently stated the goal clearly and succinctly: "The Internet must be a safe, trusted platform for the lawful distribution of content."[272]

This article has canvassed a number of recent and proposed legal and policy mechanisms to achieve that policy objective. One avenue is for rights holders to bring private actions aimed at shutting down existing and anticipated web sites that sell counterfeit products and distribute infringing content online. However, actions against such rogue sites are costly, time-consuming, and all too often futile because of the rapid pace of infringing activity over the Internet. Another approach is for the government to use public resources and procedures under current law to target such sites. Under Operation in Our Sites, the U.S. government has seized the domain names of rogue websites offering or linking to suspected infringing content. Unfortunately, rogue websites based and operated in foreign jurisdictions effectively remain out of reach of U.S. enforcement authorities. To fill such gaps in the law, legislation such as COICA and PIPA has been proposed to provide recourse against foreign rogue websites.

There is broad agreement that pursuing websites offering counterfeit goods and infringing content will require new legal tools and tactics. However, the policy implications of each proposal have come under close scrutiny in the public arena. One option is to take action against payment service providers such as credit card companies, effectively cutting off the revenue to the rogue website. Another tactic under consideration is to prevent advertising networks from placing ads on or for rogue websites. Finally, careful attention is being given to proposals that would require the blocking of domain names to curb online piracy and counterfeiting. Opponents of the use of the domain name blocking raise, among other things, First Amendment and due process concerns, while proponents argue that the practice is constitutional and a highly effective means to deter illegal online activity. All, however, agree that the right policy balance must be found to ensure that the Internet realizes its

---

[272] FCC, CONNECTING AMERICA: THE NATIONAL BROADBAND PLAN 58 (2010), http://commcns.org/sCCj9m.

full potential as a platform for the lawful distribution of creative works, to the benefit of American creators, consumers, and businesses.