

# Pace Intellectual Property, Sports & Entertainment Law Forum

---

Volume 2  
Issue 1 *Spring 2012*

Article 2

---

April 2012

## Combating Online Trademark and Copyright Infringement: ICE and DOJ Domain Name Seizures New Tools In the Government's Efforts to Combat Online IP Infringement

Tanya Dunbar

Follow this and additional works at: <https://digitalcommons.pace.edu/pipself>



Part of the [Intellectual Property Law Commons](#), and the [Internet Law Commons](#)

---

### Recommended Citation

Tanya Dunbar, *Combating Online Trademark and Copyright Infringement: ICE and DOJ Domain Name Seizures New Tools In the Government's Efforts to Combat Online IP Infringement*, 2 Pace. Intell. Prop. Sports & Ent. L.F. 43 (2012).

DOI: <https://doi.org/10.58948/2329-9894.1006>

Available at: <https://digitalcommons.pace.edu/pipself/vol2/iss1/2>

This Article is brought to you for free and open access by the School of Law at DigitalCommons@Pace. It has been accepted for inclusion in Pace Intellectual Property, Sports & Entertainment Law Forum by an authorized administrator of DigitalCommons@Pace. For more information, please contact [dheller2@law.pace.edu](mailto:dheller2@law.pace.edu).

---

## Combating Online Trademark and Copyright Infringement: ICE and DOJ Domain Name Seizures New Tools In the Government's Efforts to Combat Online IP Infringement

### Abstract

The ICE seizures and proposed legislations to codify ICE-style seizures have led many to question the legitimacy of ICE's seizures and decry the bills as censorship. Tanya Dunbar's article explores the reasons for the government's actions, the seizure mechanism the government employs, and the controversy surrounding domain name seizures. Where possible, the Ms. Dunbar offers solutions to some of the controversial issues that may arise.

### Keywords

trademark, copyright, domain names

### Cover Page Footnote

Tanya Dunbar is a recent graduate of the University of California, Hastings College of the Law located in San Francisco, California. While at UC Hastings, Dunbar completed a concentration in Intellectual Property. She was admitted to the California Bar in December 2011.

Prior to law school, Dunbar earned her B.S. in Microbiology and minor in Biochemistry from the University of the Sciences in Philadelphia, formerly, the Philadelphia College of Pharmacy and Sciences. She was drawn to the study of law upon learning about the intersection of law and science, specifically with biotechnology patents. Dunbar desired to be at the forefront of shaping legislation for such cutting-edge technology. Her initial interest in biotechnology patents has since blossomed into a love of all areas of IP.

# Combating Online Trademark and Copyright Infringement: ICE and DOJ Domain Name Seizures New Tools in the Government's Efforts to Combat Online IP Infringement

Tanya Dunbar<sup>\*</sup>

## Table of Contents

		<b>Page</b>
I.	Introduction . . . . .	45
II.	The Government's Rationale . . . . .	47
	A. <i>Caveat Emptor</i> . . . . .	47
	B. Piracy Costs Americans Jobs and Money. . . . .	48
	C. Piracy Poses a National Security Threat. . . . .	50
III.	Intellectual Property Rights Enforcement . . . . .	51
	A. RICO Authorizes Seizures For Criminal Intellectual Property Rights Infringement. . . . .	51
	B. ICE's Authority to Conduct Domain Name Seizures Stems From the Homeland Security Act of 2002. . . . .	53
	C. The DOJ Plays a Collaborative Role in Protecting Intellectual Property. . . . .	53
IV.	ICE Seizures . . . . .	54
	A. ICE Seizure Procedure, generally . . . . .	54
	B. Operation In Our Sites . . . . .	56
V.	Legislating Enforcement . . . . .	60
	A. COICA: Codifying Domain Name Seizures . . . . .	60
	B. COICA Procedure . . . . .	60
	C. PROTECT IP Act of 2011 . . . . .	61

---

<sup>\*</sup> JD Recipient 2011 from University of California, Hastings College of the Law. The author wishes to thank: Dr. Dana Beldiman for helping with topic selection; Professor Robin Feldman for her wonderful instruction and insight; and classmates in Professor Feldman's Spring 2011 Intellectual Property Concentration Capstone Seminar for their amazing input.

	D.	The House's Response to PROTECT IP – SOPA and OPEN . . . . .	62
VI.		The Debate . . . . .	63
	A.	The Proposed Legislation and ICE Seizures Are Overbroad and May Curtail Freedom of Speech and Due Process Rights. . . . .	64
		1. Due Process Requires at Least a Prompt Post-Seizure Opportunity to Be Heard. . . . .	66
		2. While the Government's Initial Seizures Might Have Been Valid, Administrative Delay May Be Having the Effect of Improperly Censoring Protected Speech. . . . .	67
	B.	Domain Name Seizures Are Ineffective As Owners Can So Easily Move Domain Names to Different Domains After Seizure; Seizures Are Therefore a Waste of Resources. . . . .	68
	C.	Interference With the DNS Is Potentially Harmful to the Internet.	70
	D.	Domain Name Seizures Could Be One Useful Tool For Protecting IPR Owners.	72
VII.		Conclusion . . . . .	72

## I. INTRODUCTION

Modern technology makes it easier and easier to reproduce and distribute counterfeit goods. Unfortunately, the law has been slow to catch up with the speed of technological progress. As a result, the Internet is supplementing brick and mortar facilities and street stands as a conduit for dispensing counterfeit goods. For instance, as music, film, and software content providers move towards purely digital products, the rate of illegal copying and distribution of these goods on the Internet is likely to surpass traditional modes. Intellectual property rights<sup>1</sup> (“IPR”) holders have always needed to be vigilant about protecting their rights, and the development of the virtual marketplace has made their job exponentially harder. It is impossible for IPR holders to police every one of the millions of Internet sites. This forces IPR owners to make tactical decisions like selectively monitoring the most egregious sites for infringing activity. Unfortunately, it is sometimes unfeasible to even monitor the most egregious sites because of their volume of content.

The market for copyrighted and/or trademarked goods, such as movies and luxury products, is very large. Websites selling, or otherwise, illegally distributing these goods stand to make significant profits, presumably at the expense of the IPR owners. By some estimates, American businesses lose more than \$25.6 billion annually because of piracy.<sup>2</sup> Although the exact figures are highly contested, it seems safe to assume that American businesses are losing significant amounts of capital from piracy. To compound the issue, there are apparently links between piracy and organized crime and even terrorism.<sup>3</sup> Because of the commercial and

---

<sup>1</sup> For the purpose of this paper, any discussion of IPR will focus on trademarks and copyrights.

<sup>2</sup> Daniel Castro, *Better Enforcement of Online Copyright Would Help, Not Harm, Consumers*, INFO. TECH. & INNOVATION FOUND. (Oct. 2010), <http://eric.ed.gov/PDFS/ED512451.pdf> [hereinafter Better Enforcement]; *Senators Introduce Bipartisan Bill to Combat Online Infringement*, Patrick Leahy (Sept. 20, 2010), [http://leahy.senate.gov/press/press\\_releases/release/?id=e26c01c9-e291-4bd3-9912-80dca46a75f6](http://leahy.senate.gov/press/press_releases/release/?id=e26c01c9-e291-4bd3-9912-80dca46a75f6) [hereinafter Leahy].

<sup>3</sup> Gregory F. Treverton, et al., *Film Piracy, Organized Crime, and Terrorism* (RAND 2009) [hereinafter RAND].

national security ramifications of Internet piracy on Americans, the United States (“U.S.”) government saw fit to protect American consumers and businesses from Internet piracy.

The U.S. Immigration and Customs Enforcement (“ICE”) has taken the lead in pursuing online piracy. Since summer 2010, ICE has seized over three hundred domain names deemed as instruments of piracy. In fall 2010, a group of senators introduced a bill known as the Combating Online Infringement and Counterfeits Act (“COICA”) into Congress. COICA would have empowered the U.S. Department of Justice (“DOJ”) to perform the type of domain name seizure actions ICE had begun, with some important expansions. Under COICA, the DOJ would be able to act not just against domain name owners, but also against third parties, like advertisers and credit card companies, to force them to cease dealing with subject domains. COICA failed to pass during that session, so its proponents later resurrected it as the Preventing Real Online Threats to Economic Creativity and Theft of Intellectual Property Act (“PROTECT IP”). PROTECT IP retains the essence of COICA while expanding the government’s power to act against foreign websites. In late 2011, a group of congressional members introduced the House version of PROTECT IP, entitled the Stop Online Piracy Act (“SOPA”). SOPA promises to extend the DOJ’s power, *inter alia*, by allowing the DOJ to also act against domestic sites.

The ICE seizures and proposed legislations to codify ICE-style seizures have led many to question the legitimacy of ICE’s seizures and decry the bills as censorship. This paper will explore the reasons for the government’s actions, the seizure mechanism the government employs, and the controversy surrounding domain name seizures. Where possible, the author will offer solutions to controversial issues.

## II. THE GOVERNMENT'S RATIONALE

While the growth of the digital marketplace has opened up new markets and added great convenience for businesses and consumers alike, it also brought with it new forms of piracy and counterfeiting.<sup>4</sup> Piracy is defined as “[t]he unauthorized and illegal reproduction or distribution of materials protected by copyright, patent, or trademark law.”<sup>5</sup> Counterfeiting is the unlawful forging, copying, or imitation of items.<sup>6</sup> “Counterfeiting includes producing or selling an item that displays a reproduction of a genuine trademark, usually to deceive buyers into thinking they are purchasing genuine merchandise.”<sup>7</sup> The author will generally use piracy to refer to both counterfeiting and criminal copyright infringement.

### A. Caveat Emptor.

Before the Internet, the available tools for copying, advertising, and distributing limited pirates in the volume of contraband they could produce and the range of potential customers. The Internet now allows pirates to reach potential purchasers globally, simply by creating websites. These websites might have domain names that are likely to confuse the user into wrongly believing the goods originate from a certain source, like [louis-vuitton-outlet-store.com](http://louis-vuitton-outlet-store.com) and [burberryoutletshop.com](http://burberryoutletshop.com).<sup>8</sup> This is worrisome because consumers are less wary about purchasing sensitive products, such as prescription medications, online.<sup>9</sup> There have been several incidents of people selling counterfeit prescription medications through the Internet.<sup>10</sup> In

---

<sup>4</sup> Leahy, *supra* note 2.

<sup>5</sup> BLACK'S LAW DICTIONARY 1186 (8th Ed. 2004) [hereinafter Black's].

<sup>6</sup> *Id.* at 376.

<sup>7</sup> *Id.*

<sup>8</sup> Office of Public Affairs, *LIST OF DOMAIN NAMES SEIZED BY ICE*, ICE.GOV (Nov. 29, 2010), *available at* [http://www.ice.gov/doclib/news/releases/2010/domain\\_names.pdf](http://www.ice.gov/doclib/news/releases/2010/domain_names.pdf) [hereinafter 82 Domain List].

<sup>9</sup> Leahy, *supra* note 2.

<sup>10</sup> 60 MINUTES: *The Fight Against Counterfeit Drugs* (CBS television broadcast Mar. 13, 2011), *available at* <http://www.cbsnews.com/video/watch/?id=7359537n#ixzz1MI1223cf> [hereinafter 60 Minutes].

at least one of those cases, the vendor sold counterfeit cancer drugs to unwitting cancer patients.<sup>11</sup> In another case, an Arizona couple offered more than 600 Food and Drug Administration (“FDA”) approved drugs, including blockbusters such as Viagra, Celebrex, and Lipitor, at deep discounts through their Website and toll-free telephone lines.<sup>12</sup> The couple would then fill orders with non-FDA approved imitations from India.<sup>13</sup> The couple admitted that from 2004 to 2006 their illegal prescription drug business generated revenues of more than \$2,500,000.<sup>14</sup>

B. Piracy Costs Americans Jobs and Money.

Pirated digital content accounts for a significant percentage of Internet traffic. One recent study released by Envisional, a British anti-piracy consultant, concluded that the illegal uploading or downloading of copyrighted material of a non-pornographic nature accounts for seventeen percent of U.S. web traffic and almost a quarter globally.<sup>15</sup> Given the volume of online piracy, it is logical to conclude that this piracy will have some negative effect on IPR owners. The exact effect, of course, is debatable as there is no consensus on the methodology for assessing piracy rate and any subsequent harm to IPR owners.<sup>16</sup> The government and IPR

---

<sup>11</sup> *Canadian Man Pleads Guilty to Selling Counterfeit Cancer Drugs Using the Internet*, UNITED STATES DEPARTMENT OF JUSTICE (May. 11, 2010), <http://www.justice.gov/opa/pr/2010/May/10-ag-554.html>.

<sup>12</sup> *Lake Havasu City Couple Plead Guilty in Indian Prescription Drug Import Case*, SEATTLE TIMES (Mar. 17, 2009), [http://seattletimes.nwsources.com/html/nationworld/2008876851\\_apinternetdrugs.html](http://seattletimes.nwsources.com/html/nationworld/2008876851_apinternetdrugs.html) [hereinafter Lake Havasu].

<sup>13</sup> *Kingman Couple Sentenced for Fraudulently Distributing Indian-Manufactured Counterfeit Drugs*, UNITED STATES DEPARTMENT OF JUSTICE (May. 25, 2010), <http://www.justice.gov/criminal/cybercrime/frenchSent.pdf> [hereinafter Kingman].

<sup>14</sup> *Id.*

<sup>15</sup> *Technical report: An Estimate of Infringing Use of the Internet*, ENVISIONAL LTD. (Jan. 2011), [http://documents.envisional.com/docs/Envisional-Internet\\_Usage-Jan2011.pdf](http://documents.envisional.com/docs/Envisional-Internet_Usage-Jan2011.pdf). [hereinafter Envisional]. NBC Universal commissioned the study in order to determine the extent of online copyright infringement and how much bandwidth pirated works take up online.

<sup>16</sup> See Daniel Castro, *et al*, *Steal These Policies: Strategies for Reducing Digital Piracy*, INFO. TECH. & INNOVATION FOUND. (2009) FN 7, <http://www.itif.org/files/2009-digital-piracy.pdf> [hereinafter Steal These], arguing: Measuring losses due to piracy is an imperfect science because pirated products are not perfect substitutes for legally purchased goods. First, the actual rate of piracy is uncertain. Even if researchers could agree on the rate of piracy, they would still need to decide how many of the pirated products would have been purchased legally if piracy were not an option. “Some studies assume a one-to-one substitution, all pirated material would have been purchased and thus



owners use rhetoric like, “theft” and “stealing” to underscore their contention that piracy is a crime against rights holders, while detractors argue that the government’s numbers are inflated.<sup>17</sup>

While Internet piracy is a problem for many nations with IP-related industries, it is a particular problem for the U.S. because IP constitutes a large proportion of the U.S. economy. According to Victoria Espinel, the U.S. Intellectual Property Enforcement Coordinator, “Americans produce more technologies, more brands, more creative works and more innovation than any other nation on Earth.”<sup>18</sup> The U.S. Chamber of Commerce<sup>19</sup> estimates that American IP accounts for more than \$5 trillion of the country’s gross domestic product (“GDP”)<sup>20</sup>, and IP-intensive industries employ more than 18 million workers.<sup>21</sup> Online piracy and the sale of counterfeit goods are believed to cost American businesses billions of dollars annually, and result in hundreds of thousands of lost jobs.<sup>22</sup> The American Federation of Labor and Congress of Industrial Organizations (“AFL-CIO”) estimates that digital theft of movies and music alone costs more than 200,000 jobs.<sup>23</sup> As IP-related industries form a core part of America’s

---

the market value of pirated goods represents the actual loss, an overly optimistic assumption.” Other studies take a different approach and use surveys to determine what percentage of those who use pirated material would have purchased these goods if piracy were not an option.

<sup>17</sup> Leahy, *supra* note 2. See Andrew Keen, *Dust-Up: What’s the true impact of illegal downloading on jobs and the arts?* LOS ANGELES TIMES OPINION (Mar. 17, 2011), <http://opinion.latimes.com/opinionla/2011/03/dust-up-when-it-comes-to-piracy-can-new-laws-rather-than-new-approaches-do-more-harm-than-good-round.html>.

<sup>18</sup> *Justice Department Announces New Intellectual Property Task Force as Part of Broad IP Enforcement Initiative*, UNITED STATES DEPARTMENT OF JUSTICE (Feb. 12, 2010), <http://www.justice.gov/opa/pr/2010/February/10-ag-137.html> [hereinafter DOJ IPTF].

<sup>19</sup> The U.S. Chamber of Commerce is the world’s largest business federation representing the interests of more than three million American businesses. It is an advocate of free enterprise. *About the U.S. Chamber of Commerce*, U.S. CHAMBER, <http://www.uschamber.com/about> (last visited Mar. 27, 2012).

<sup>20</sup> Estimated total GDP for 2010 was approximately \$15 trillion. *National Income and Product Accounts Gross Domestic Product, 4th Quarter and Annual 2010 (advance estimate)*, BUREAU OF ECONOMIC ANALYSIS (Jan. 28, 2011), [http://www.bea.gov/newsreleases/national/gdp/2011/gdp4q10\\_adv.htm](http://www.bea.gov/newsreleases/national/gdp/2011/gdp4q10_adv.htm).

<sup>21</sup> Leahy, *supra* note 2.

<sup>22</sup> *Id.*

<sup>23</sup> *Id.*; see also, DPE Research Department, Fact Sheet 2010 – *Intellectual Property Theft: A Threat to U.S. Workers, Industries, and Our Economy*, DPEAFLCIO (Aug. 2010), available at [http://dpeaflcio.org/pdf/DPE-fs\\_2010\\_intellectual\\_prop.pdf](http://dpeaflcio.org/pdf/DPE-fs_2010_intellectual_prop.pdf).

competitive advantage, creating higher wage jobs and export sales that help offset the large trade deficit, their decline would logically have disastrous consequences.<sup>24</sup>

C. Piracy Poses a National Security Threat.

The government and proponents of pending legislation seem to believe that piracy is linked to organized crime and terrorism. Skeptics counter that the figures the government relies on in reaching this conclusion are overinflated and stem from efforts by groups like the Motion Picture Association of America (“MPAA”), to link film piracy with national security.<sup>25</sup> In one 2009 study funded by the MPAA, the RAND Statistics Group<sup>26</sup> concluded that organized crime and terrorism are financed by pirated digital video discs (“DVD”) sales.<sup>27</sup> The report authors concluded that countless mobsters from around the world and in a variety of gangs have relied upon pirated goods to fund illegal activities.<sup>28</sup> For anyone who has seen a gangster movie, this conclusion seems commonsensical as organized crime units generally seek fast money by any means possible; there is no reason to suggest IP crimes would be excluded. Similarly, organized terrorists cells need to fund their operations and piracy seems like a simple enough option. In fact, news stories have shown that terrorists groups and crime syndicates are engaged in counterfeiting IP-related goods.<sup>29</sup>

---

<sup>24</sup> Steal These, *supra* note 16 at 4.

<sup>25</sup> Mike Masnick, *Hey NY Times: Can You Back Up The Claim Of \$200 Billion Lost To Counterfeiting?*, TECH DIRT (Aug. 2, 2010), <http://www.techdirt.com/articles/20100801/17431810439.shtml>; see Betsy Schiffman, *Is CD Piracy a Matter for Homeland Security?*, DAILY FINANCE (Apr. 20, 2010), <http://www.dailyfinance.com/2010/04/20/is-cd-piracy-a-matter-for-homeland-security/> [hereinafter CD Piracy].

<sup>26</sup> The RAND Corporation is a nonprofit research organization. Their research is commissioned by a global clientele that includes government agencies, foundations, and private-sector firms. They then make research results available to the general public. See *RAND at a Glance*, RAND CORPORATION (Mar. 14, 2012), <http://www.rand.org/about/glance.html>.

<sup>27</sup> RAND, *supra* note 3 (study authors were adamant about their independence).

<sup>28</sup> CD Piracy, *supra* note 25.

<sup>29</sup> Jon Ungood-Thomas, *Designer fakes ‘are funding Al-Qaeda’*, THE SUNDAY TIMES (Mar. 20, 2005), <http://www.timesonline.co.uk/tol/news/uk/article432410.ece>; see *Counterfeit Bags May Have Links To Organized Crime, Terrorism – Kate Spade’s Attorney Going After House Parties*, WISN.COM (May 8, 2003),

### III. INTELLECTUAL PROPERTY RIGHTS ENFORCEMENT

IPR can be enforced in several ways. The IPR owner might bring a lawsuit against an alleged infringer.<sup>30</sup> Also, in certain circumstances, a variety of federal agencies, such as DOJ, ICE and U.S. Customs and Border Protection (“CBP”), may become involved in IP rights enforcement.<sup>31</sup> Since much of the debate surrounding ICE’s seizures question the agency’s authority, it is necessary to delve into the history of the agency and its legislatively enumerated powers in order to get a clearer understanding of its proffered basis for the seizures.

#### A. RICO Authorizes Seizures For Criminal Intellectual Property Rights Infringement.

In response to an increasing wave of counterfeit activity,<sup>32</sup> Congress in 1996 increased penalties and facilitated procedures for the anti-counterfeiting battle.<sup>33</sup> One aspect of the 1996 Act was to increase criminal penalties by making trafficking in certain IP contraband a Racketeer Influenced and Corrupt Organizations Act (“RICO”) predicate offense, thereby triggering RICO coverage.<sup>34</sup> The 1996 Act amended 18 U.S.C.A. § 1961(1)(B) by inserting as predicate offenses: criminal use of counterfeit labels for phonorecords, computer programs and motions pictures, 18 U.S.C. § 2318; *criminal infringement of copyright*, 17 U.S.C. § 506 and 18 U.S.C. § 2319; and *criminal trademark counterfeiting* under 18 U.S.C. § 2320.<sup>35</sup>

---

<http://www.wisn.com/news/2191330/detail.html#ixzz1MGiASYPL> (Genovese crime family was indicted for selling counterfeit handbags).; see *Counterfeit goods are linked to terror groups - Business International Herald Tribune*, N.Y. TIMES (Feb. 12, 2007), <http://www.nytimes.com/2007/02/12/business/worldbusiness/12iht-fake.4569452.html>.

<sup>30</sup> Brian T. Yeh, *Intellectual Property Rights Violations: Federal Civil Remedies and Criminal Penalties Related to Copyrights, Trademarks, and Patents*, (Cong. Res. Serv, Oct. 31, 2008) (available at <http://www.fas.org/sgp/crs/misc/RL34109.pdf>) [hereinafter Yeh].

<sup>31</sup> Yeh, *supra* note 30.

<sup>32</sup> See The International Trademark Association Summary Statement on H.R. 2511, JUDICIARYHOUSE.GOV, <http://judiciary.house.gov/Legacy/475.htm> (last visited Mar. 27, 2012).

<sup>33</sup> J. Thomas McCarthy, McCarthy on Trademarks and Unfair Competition 75, § 30:37 (4th ed. 2004) [hereinafter McCarthy].

<sup>34</sup> *Id.* (RICO is more commonly used for property related to drugs.)

<sup>35</sup> *Id.*

RICO, via 18 U.S.C. § 2323, allows the government to seize and seek forfeiture not only of counterfeit goods, goods that criminally infringe copyright, or the financial proceeds of those goods, but also the non-monetary assets associated with those goods.<sup>36</sup> Seizure is the initial taking of property into the government's custody to establish jurisdiction for a civil *in rem* proceeding, while, forfeiture is the final deprivation of the property without compensation.<sup>37</sup> RICO authorizes the government to seize property without prior notice in order to preserve evidence for later prosecution.<sup>38</sup> Forfeiture fosters the government's interest in preventing continued illicit use of property and in enforcing criminal sanctions.<sup>39</sup> This seems especially necessary in the case of websites because they can easily be moved outside of U.S. jurisdiction.

Domain names used to market or distribute pirated merchandise could qualify as property associated with a criminal IP infringement enterprise, and therefore subject to seizure and possible forfeiture. This is quite evident when dealing with sites like *louis-vuitton-outlet-store.com* and *burberryoutletshop.com* whose only purpose appears to be disseminating counterfeit goods. The analysis becomes significantly more nuanced for sites featuring both infringing and non-infringing content or that simply link to sites that carry infringing content.

---

<sup>36</sup> McCarthy, *supra*, note 33.

<sup>37</sup> Terry Hart, *ICE Seizures Criticism: Magic Words*, COPYHYPE (Mar. 21, 2011), <http://www.copyhype.com/2011/03/ice-seizures-criticism-magic-words/> (citing *Marine Midland Bank v. United States*, 11 F.3d 1119, 1124 (2nd Cir. 1993) and *The Brig Ann*, 13 U.S. 289, 291 (1815)) [hereinafter Magic Words].; *Id.* (forfeitures, unlike seizures, are subject to Eight Amendment limitations against excessive fines (citing *United States v. Bajakajian*, 524 U.S. 321 (1998))).

<sup>38</sup> McCarthy, *supra* note 33.

<sup>39</sup> Terry Hart, *Feds Seize Domain Names*, COPYHYPE (Dec. 6, 2010), <http://www.copyhype.com/2010/12/feds-seize-domain-names/> [hereinafter Feds Seize].

B. ICE's Authority to Conduct Domain Name Seizures Stems From the Homeland Security Act of 2002.

On November 25, 2002, President Bush signed the Homeland Security Act of 2002 into law.<sup>40</sup> As a result, since March 1, 2003, the former Immigration and Naturalization Service (“INS”) of the DOJ and the former U.S. Customs Service of the Department of the Treasury were transferred to the Department of Homeland Security (“DHS”) and reorganized as CBP, ICE, and U.S. Citizenship and Immigration Services (“USCIS”).<sup>41</sup> In total, DHS is composed of 22 entities; ICE performs the traditional customs services.<sup>42</sup> Under the new regime:

Any officer of [CBP] or [ICE] may seize and forfeit any property that has been or is being used in the commission of a violation of any statutory authority involving the unlawful introduction of aliens, contraband or proceeds of such introduction, pursuant to, but not limited to, section 274(a) of the Act (8 U.S.C. 1324(a)).<sup>43</sup>

Effective June 30, 2010, seizures and forfeitures are carried out according to 19 CFR parts 162 and 171.<sup>44</sup> This amendment introduced some due process protections by permitting “CBP to entertain petitions for remission and return of seized property prior to completing the forfeiture process,” regardless of the basis of the seizure and which agency conducted it.<sup>45</sup>

C. The DOJ Plays a Collaborative Role in Protecting Intellectual Property.

In early 2010, U.S. Attorney General (“AG”) Eric Holder announced the formation of a new DOJ Task Force on Intellectual Property (“Task Force”) chaired by the Deputy AG.<sup>46</sup> The Task Force works to coordinate federal efforts to combat infringement with state and local law

---

<sup>40</sup> Administrative Process for Seizures and Forfeitures Under the Immigration and Nationality Act and Other Authorities, FEDERAL REGISTER (Feb. 19, 2008), <http://federalregister.gov/a/E8-2965> [hereinafter Administrative Process].

<sup>41</sup> Administrative Process, *supra*, note 40.

<sup>42</sup> CD Piracy, *supra* note 25.

<sup>43</sup> 8 C.F.R. § 274.1 (2008).

<sup>44</sup> 8 C.F.R. § 274 (2008) and Administrative Process, *supra* note 40.

<sup>45</sup> Administrative Process, *supra* note 40.

<sup>46</sup> DOJ IPTF, *supra* note 18.

enforcement partners, as well as international counterparts.<sup>47</sup> One major focus of the Task Force is “exploring the international aspects of intellectual property enforcement, including the links between IP crime and international organized crime.”<sup>48</sup> The Task Force will continue working with federal agencies, such as DHS and the Federal Communications Commission.<sup>49</sup>

#### IV. ICE SEIZURES

##### A. ICE Seizure Procedure, Generally

ICE looks at certain factors when identifying sites for seizure. First, ICE considers the commercial nature of the site by investigating ad revenue, subscriptions, and sales.<sup>50</sup> ICE also considers whether the site is purely engaged in IP infringement and the popularity and influence of the site.<sup>51</sup> In order to exercise *in rem* jurisdiction, ICE also looks for a nexus between the site and the U.S., such as whether site owners sell or provide infringing content to Americans.<sup>52</sup> ICE establishes that the targeted site is engaged in criminal activity by conducting test-buys, streaming, or downloading infringing content.<sup>53</sup> Often, self-interested groups, such as MPAA, alert ICE to the questionable domain names.<sup>54</sup> Considering how much time and energy rights holders probably spend policing their IP, it is logical that they would be more aware of the infringement landscape than the government.

---

<sup>47</sup> *Id.*

<sup>48</sup> *Id.*

<sup>49</sup> *Id.*

<sup>50</sup> *Operation In Our Sites*, NATIONAL INTELLECTUAL PROPERTY RIGHTS COORDINATION CENTER, [https://www.yousendit.com/directDownload?phi\\_action=app/directDownload&fl=SWhZekZqQ0M4Q1RvS3B1bTBkQ09SMHVDeVNFRkF0Qm1kRmM2aXU1dg](https://www.yousendit.com/directDownload?phi_action=app/directDownload&fl=SWhZekZqQ0M4Q1RvS3B1bTBkQ09SMHVDeVNFRkF0Qm1kRmM2aXU1dg) (last visited Mar. 27, 2012) [hereinafter Chamber].

<sup>51</sup> *Id.*

<sup>52</sup> *Id.*

<sup>53</sup> Complaint at 4-14, *United States v. TVShack.net et. al.*, No. 10 CV 9203 (S.D.N.Y. Dec. 3, 2010), available at <http://www.copyright.com/2010/12/tvshack-forfeiture-complaint/> [hereinafter TVShack Complaint].

<sup>54</sup> Application and Affidavit for Seizure Warrant at 11, *United States v. Rapgodfather.com et. al.*, No. 10-2822M (C.D. Cal. Nov. 17, 2010), available at <http://www.docstoc.com/docs/67610787/45705510-Operation-in-Our-Sites-2-0> [hereinafter Operation 2.0].

Once ICE obtains evidence that a site is engaged in IP infringement, ICE agents file applications and affidavits for seizure warrants in a district court asserting seizure under 18 U.S.C. §2323(a)(1)(A) – (B) and 981(b), due to a violation of 17 U.S.C. §506(a) and 18 U.S.C. §2319 for criminal copyright infringement.<sup>55</sup> Presumably, the government also uses 18 U.S.C. §2320, criminal trademark infringement, as a basis for seeking warrants where counterfeit goods are at issue, however, this author could locate no such court filings, only ICE’s statements regarding serving court orders to websites illegally selling and distributing counterfeit goods.<sup>56</sup>

Section 2323 generally provides that any property used, or intended to be used to commit or facilitate criminal copyright infringement or criminal trademark infringement is subject to criminal and civil forfeiture to the U.S. government.<sup>57</sup> The requirements for civil forfeiture are laid out in 18 U.S.C. §981(b), namely, a warrant upon a showing of probable cause.<sup>58</sup> The seizure warrant is presented to personnel of the domain name registrars<sup>59</sup> and the domain name<sup>60</sup> registry,<sup>61</sup> who will be directed to restrain and lock the subject domain names for which it serves as a “top-level domain”<sup>62</sup> (“TLD”) name registry, pending transfer of all rights, title, and interest

---

<sup>55</sup> Affidavit in Support of Application for Seizure Warrant at 44, *United States v. HQ-Streams.com et. al.*, No. 11 MAG 262 (S.D.N.Y Jan 31, 2011) available at <http://www.scribd.com/doc/48065720/United-States-v-hq-streams-com-et-al-Affidavit-in-Support-of-Application-for-Seizure-Warrant> [hereinafter Operation 3.0].

<sup>56</sup> *Homeland Security Investigations brings counterfeit designers to heel*. IMMIGRATION CUSTOMS ENFORCEMENT ICE (July. 28, 2011), <http://www.ice.gov/news/releases/1107/110728washingtondc.htm>. [hereinafter Shoe Clerk]

<sup>57</sup> 18 U.S.C. § 2323 (2006).

<sup>58</sup> 18 U.S.C. § 981(b) (2006).

<sup>59</sup> Registrars serve as middlemen between purchasers of domain names and the registries. The purchaser or registrant controls the IP address and subsequently the computer to which it resolves. The registrant can therefore move his domain name to another computer anywhere in the world. Operation 2.0, *supra* note 54 at 5. See also Marshall Brain & Stephanie Crawford, *How Domain Servers Work*, HOWSTUFFWORKS?RKS, <http://computer.howstuffworks.com/dns.htm> (last visited Mar. 27, 2012).

<sup>60</sup> A domain name is a simple, easy to remember way for humans to identify computers on the Internet using a series of characters. It corresponds to a specific Internet Protocol address. Domain names consist of one or more parts or labels, delimited by periods. For example, [www.example.com](http://www.example.com). See Marshall Brain & Stephanie Crawford, *How Domain Servers Work*, HOWSTUFFWORKS?RKS, <http://computer.howstuffworks.com/dns.htm> (last visited Mar. 27, 2012).

<sup>61</sup> A single company, called a registry, determines which Second-Level Domain (“SLD”) resolves to a single IP address. Operation 2.0, *supra* note 54, at 5.

<sup>62</sup> The hierarchy of domains goes from right to left, with each label to the left specifying a subdivision or subdomain of the domain on the right. The right most labels, i.e. COM, EDU, GOV AND ORG, are the top-level domain (“TLD”) names. As an example, [www.example.com](http://www.example.com) means the computer assigned that name is in the COM TLD,

in the subject domain names to the U.S. upon completion of forfeiture proceedings.<sup>63</sup> Upon seizure, the registry must reroute the domain names to the Internet Protocol<sup>64</sup> (“IP”) address 74.81.170.110, where the government displays a website with a notice that the domain name was seized by ICE – Homeland Security Investigations (“HSI”).<sup>65</sup> This process does not provide any advanced notice to the subject domain name owners. Interested parties have sixty days to challenge the forfeiture once ICE files a forfeiture claim.<sup>66</sup>

B. Operation In Our Sites

Buoyed by its newfound authority, on June 30, 2010, ICE and the U.S. Attorney for the Southern District of New York (“SDNY”) announced the launch of “Operation In Our Sites,” a program designed to investigate and prosecute Internet piracy and counterfeiting.<sup>67</sup> In Operation In Our Sites 1.0 (“Operation 1.0”), authorities executed seizure warrants against ten domain names of websites believed to be offering first-run movies during June of 2010.<sup>68</sup> Eight of those sites were targeted for seizure by the SDNY.<sup>69</sup> Agents from ICE-HSI “also seized assets from 15 bank, Paypal, investment and advertising accounts, and executed four residential search warrants

---

and the “example” second-level domain (“SLD”), and the computer is on the web server. Operation 2.0, *supra* note 54 at 5. “There are several hundred TLDs, Within every TLD there is a huge list of SLDs. For example, in the COM TLD, howstuffworks and yahoo. Every name in the COM TLD must be unique, but there can be duplication across domains. For example, howstuffworks.com and howstuffworks.org are completely different machines. The left-most word, such as www or encarta, is the host name. It specifies the name of a specific machine (with a specific IP address) in a domain.

<sup>63</sup> Operation 2.0, *supra* note 54 at Attachment A.

<sup>64</sup> Every computer has an IP address. An IP address is a set of four numbers, each in the range of 0-255, separated by periods. It is analogous to a home or business street address because it enables computers connected to the Internet to properly route traffic to each other. Generally, Internet Service Providers (“ISPs”) assign IP addresses to users. Domain Name Servers (“DNS”) translate domain names users enter into their browser’s address bar into IP addresses readable by computers. See Marshall Brain & Stephanie Crawford, *How Domain Servers Work*, HOWSTUFFWORKS, <http://computer.howstuffworks.com/dns.htm> (last visited Mar. 27, 2012).

<sup>65</sup> Operation 2.0, *supra* 54 at 71 and Attachment A

<sup>66</sup> Mike Masnick, *Homeland Security Finally Files For Civil Forfeiture Of Domains Seized Back In June*, TECH DIRT (Jan. 3, 2011), <http://www.techdirt.com/articles/20101230/15591512476/homeland-security-finally-files-civil-forfeiture-domains-seized-back-june.shtml> [hereinafter Civil Forfeiture].

<sup>67</sup> “Operation In Our Sites” targets Internet movie pirates: ICE, Manhattan U.S. Attorney seize multiple Web sites for criminal copyright violations, IMMIGRATION CUSTOMS ENFORCEMENT ICE (June 30, 2010), <http://www.ice.gov/news/releases/1006/100630losangeles.htm> [hereinafter ICE launch].

<sup>68</sup> *Id.*

<sup>69</sup> *Id.*



in several states.”<sup>70</sup> The National Intellectual Property Rights Coordination Center (“IPRCC”), which is led by ICE, also seized ninjavideo.net and ninjathis.net.<sup>71</sup> ICE claims that as a result of Operation 1.0, an additional 81 of the top 304 streaming websites voluntarily stopped offering illegal content or completely shut down.<sup>72</sup> ICE finally filed for civil forfeiture against seven of the ten sites on December 9, 2010.<sup>73</sup>

At a press conference on November 29, 2010, AG Eric Holder announced that as part of Operation 2.0 the DOJ, DHS and nine U.S. Attorneys’ Offices obtained and executed seizure orders against 82 domain names of websites deemed to be engaged in the sale and distribution of counterfeit goods and illegal copyrighted works.<sup>74</sup> The goods in question ranged from handbags to Digital Video Discs (“DVD”) box sets and were strategically targeted around Cyber Monday.<sup>75</sup> Although the majority of websites seemed to be blatantly trafficking in counterfeit goods, a few appeared to be music blogs and file-sharing sites – namely, rapgodfathers.com, torrent-finder.com, rmx4u.com, dajaz1.com, and onsmash.com.<sup>76</sup>

On January 31, 2011, ICE submitted an affidavit in support of a seizure warrant application to seize the following ten domain names: HQ-streams.com, HQ-streams.net, atdhe.net, firstrow.net, channelsurfing.net, ilemi.com, iilemi.com, iilemii.com, rojadirecta.org, and rojadirecta.com.<sup>77</sup> These websites were believed to illegally stream live sporting event telecasts and Pay-Per-View events, such as National Basketball Association (“NBA”) and

---

<sup>70</sup> *Id.*

<sup>71</sup> ICE Launch, *supra* note 67 The IPRCC unites the U.S. government agencies that fight IP theft. This includes ICE, CBP, Federal Bureau of Investigations (“FBI”), Food and Drug Administration (“FDA”) and others.

<sup>72</sup> Chamber, *supra* note 50.

<sup>73</sup> Namely, TVshack.net, movies-links.tv, filespump.com, now-movies.com, planetmoviez.com, thepiratecity.org, and zml.com. TVShack Complaint, *supra* note 53 at 1.

<sup>74</sup> Eric Holder, Attorney General, Speaker at the Operation in Our Sites II Press Conference (Nov. 29, 2010) (available at <http://www.justice.gov/iso/opa/ag/speeches/2010/ag-speech-101129.html>).

<sup>75</sup> 82 Domain List, *supra* note 8.

<sup>76</sup> Operation 2.0, *supra* note 54.

<sup>77</sup> Operation 3.0, *supra* note 55 at 1-47.

National Football League (“NFL”) games.<sup>78</sup> The operator of channelsurfing.net, Bryan McCarthy, was later arrested on charges of criminal copyright infringement.<sup>79</sup> Interestingly, Spanish courts had already twice declared Rojadirecta legal after a three-year legal battle in Spain.<sup>80</sup> Rojadirecta does not itself carry any copyrighted content; they only link to other sites.<sup>81</sup> The site is owned by a Spanish company, and its only connection to the U.S., other than the fact that it can be accessed from the United States, is that a U.S.-based registry operator maintains the general TLD, “.org.”<sup>82</sup>

ICE timed its fourth maneuver, aimed at websites selling counterfeit goods, for Valentines Day, 2011.<sup>83</sup> ICE seized 18 websites engaged in selling and distributing counterfeit luxury goods, like Burberry, Chanel, and Prada, as part of “Operation Broken Hearted.”<sup>84</sup> Similar to the sites targeted for Cyber Monday, most, if not all, of these domain names were used to blatantly sell counterfeit goods via the Internet. ICE’s fifth offensive took place on May 25, 2011.<sup>85</sup> The government seized five domain names they believed were being used to sell counterfeit goods and illegally distribute copyrighted content.<sup>86</sup> In *Operation In Our Sites v 6.0* on July 28, 2011, the government seized 17 domain names allegedly selling and distributing

---

<sup>78</sup> *Id.* at 6-7.

<sup>79</sup> David Makarewicz, *Arrest Of Website Operator Renews Debate Over Constitutionality of Government Domain Seizures*, SITES AND BLOGS (Mar. 9, 2011), <http://www.sitesandblogs.com/2011/03/arrest-of-website-operator-renews.html> [hereinafter Makarewicz].

<sup>80</sup> Ernesto, *U.S. Resume Controversial File-Sharing Domain Seizures (Updated)*, TORRENT FREAK BLOG (Feb. 11, 2011), <http://torrentfreak.com/us-resume-file-sharing-domain-seizures-110201/> [hereinafter TorrentFreak]

<sup>81</sup> *Id.*

<sup>82</sup> *Id.*

<sup>83</sup> *Sweetheart, but fake, deals put on ICE: “Operation Broken Hearted” protects consumers from counterfeit Valentine’s Day goods*, IMMIGRATION CUSTOMS ENFORCEMENT ICE (Feb 14, 2011), <http://www.ice.gov/news/releases/1102/110214washingtondc.htm> [hereinafter Broken Hearted].

<sup>84</sup> *Id.*

<sup>85</sup> *ICE puts the summer heat on counterfeiters PSA released last month now has nearly 100,000 views*, IMMIGRATION CUSTOMS ENFORCEMENT ICE (May 25, 2011), <http://www.ice.gov/news/releases/1105/110525washingtondc.htm>.

<sup>86</sup> *Id.*

counterfeit goods and arrested one website operator.<sup>87</sup> For the seventh phase of Operation In Our Sites, ICE pursued websites selling counterfeit sports paraphernalia, seizing 58 domain names.<sup>88</sup> The task force used Cyber Monday – November 28, 2011 – to carry out its most recent operation against websites selling counterfeit goods.<sup>89</sup> This time the government seized 150 websites.<sup>90</sup>

ICE and its collaborators have seized 350 websites to date, of which 116 have actually been forfeited to the U.S. government.<sup>91</sup> According to one source, at least five operators of seized domain names have challenged the seizures – rojadirecta.org, rojadirecta.com, Dajaz1.com, onsmash.com, and torrent-finder.com.<sup>92</sup> The court dismissed rojadirecta's suit against the government on a technicality.<sup>93</sup> Operators of the ninjavidio sites were criminally prosecuted, and all five pled guilty to conspiracy and/or criminal copyright infringement.<sup>94</sup> The government finally returned dajaz1.com to its original owners after holding the domain for over one year without instituting any forfeiture proceeding.<sup>95</sup>

---

<sup>87</sup> Shoe Clerk, *supra* note 56.

<sup>88</sup> ICE announces results of 'Operation Strike Out' – Protects consumers from counterfeit sports paraphernalia on the Internet and on the streets, IMMIGRATION CUSTOMS ENFORCEMENT ICE (Oct. 31, 2011), <http://www.ice.gov/news/releases/1110/111031washingtondc.htm>.

<sup>89</sup> Department of Justice, Federal Courts Order Seizure of 150 Website Domains Involved in Selling Counterfeit Goods as Part of DOJ, ICE HSI and FBI Cyber Monday Crackdown, UNITED STATES DEPARTMENT OF JUSTICE (Nov. 28, 2011), <http://www.justice.gov/opa/pr/2011/November/11-ag-1540.html> [hereinafter Cyber Monday].

<sup>90</sup> *Id.*

<sup>91</sup> Cyber Monday, *supra* note 89.

<sup>92</sup> Mike Masnick, *The List of Sites Challenging Domain Seizures*, TECH DIRT (June 13, 2011), <http://www.techdirt.com/articles/20110612/21573514664/list-sites-challenging-domain-seizures.shtml>.

<sup>93</sup> Mike Masnick, *Court Dismisses Puerto 80 Rojadirecta Case (For Now)... But Doesn't Give Back The Domain*, TECH DIRT (Dec. 8, 2011), <http://www.techdirt.com/articles/20111208/01424117003/court-dismisses-puerto-80-rojadirecta-case-now-doesnt-give-back-domain.shtml>.

<sup>94</sup> *Remaining Co-Founder of NinjaVideo.net Pleads Guilty to Criminal Copyright Conspiracy*, UNITED STATES DEPARTMENT OF JUSTICE (Nov. 3, 2011), <http://www.justice.gov/opa/pr/2011/November/11-crm-1449.html>.

<sup>95</sup> Mike Masnick, *Breaking News: Feds Falsely Censor Popular Blog For Over A Year, Deny All Due Process, Hide All Details...*, TECH DIRT (Dec. 8, 2011), <http://www.techdirt.com/articles/20111208/08225217010/breaking-news-feds-falsely-censor-popular-blog-over-year-deny-all-due-process-hide-all-details.shtml>.

## V. LEGISLATING ENFORCEMENT

### A. COICA: Codifying Domain Name Seizures

Senators Patrick Leahy (D-VT) and Orrin Hatch (R-UT) introduced bill S.3804<sup>96</sup> to the 111th Congress on September 20, 2010.<sup>97</sup> COICA would have empowered the DOJ to “track and shut down websites devoted to providing access to unauthorized downloads, streaming or sale of copyrighted content and counterfeit goods.”<sup>98</sup> The Senate Committee on the Judiciary (“Committee”) voted 19-0 in favor of COICA, but Senator Ronald Wyden (D-OR) blocked it from a full Senate vote.<sup>99</sup> Committee Chairman Leahy resurrected the matter in the 112th Congress,<sup>100</sup> and held hearings on IP infringement on the Internet in February of 2011.<sup>101</sup> The hearings gave birth to new legislation, Preventing Real Online Threats to Economic Creativity and Theft of Intellectual Property Act or PROTECT IP.<sup>102</sup>

### B. COICA Procedure

COICA would have given the U.S. AG power to file an *in rem* action in a federal court, requesting a court order requiring the U.S. – based registrar, such as godaddy.com, or the U.S. –

---

<sup>96</sup> Leahy, *supra* note 2; 15 U.S.C. 1116(d)). The proposed amendment would add: 18 U.S.C. § 2324, which defines “dedicated to infringing activities” as a site which is (A) primarily designed, has no demonstrable, commercially significant purpose or use other than, or is marketed by its operator, or by a person acting in concert with the operator, to offer – (i) goods or services in violation of title 17, United States Code, or enable or facilitate a violation of title 17, United States Code, (ii) to sell or distribute goods, services, or materials bearing a counterfeit mark, as that term is defined in section 34(d) of the Lanham Act.

<sup>97</sup> Better Enforcement, *supra* note 2; and Leahy, *supra* note 2.

<sup>98</sup> Leahy, *supra* note 2.

<sup>99</sup> *Senator Wyden Response to the PROTECT IP Act Introduction*, WYDEN SENATE (May 12, 2011), <http://wyden.senate.gov/newsroom/press/release/?id=8c700e16-20a6-4f57-8438-ecf700b89b87> [hereinafter Wyden Reacts].

<sup>100</sup> Emilio W. Cividanes, *et al*, *Senate Judiciary Committee holds hearing on targeting sites dedicated to stealing American intellectual property*, LEXOLOGY (Mar. 25, 2011), <http://www.lexology.com/library/detail.aspx?g=1a6be67c-55f8-427b-842f-8657066e7659> [hereinafter Cividanes].

<sup>101</sup> *Leahy Chairs Hearing On Costly Problem Of Online Infringement*, LEAHY SENATE (Feb 16, 2011), [http://www.leahy.senate.gov/press/press\\_releases/release/?id=C7641CB8-47DE-49ED-8DFD-8244E18AEDFA](http://www.leahy.senate.gov/press/press_releases/release/?id=C7641CB8-47DE-49ED-8DFD-8244E18AEDFA) [hereinafter Costly Infringement].

<sup>102</sup> *Leahy, Hatch, Grassley Unveil Targeted Bill To Counter Online Infringement*, LEAHY SENATE (May 12, 2011), [http://www.leahy.senate.gov/press/press\\_releases/release/?id=A18DDCC4-8DA6-4CB9-B46E-104C21537D50](http://www.leahy.senate.gov/press/press_releases/release/?id=A18DDCC4-8DA6-4CB9-B46E-104C21537D50) [hereinafter PROTECT IP].

based registry, like Verisign, to suspend the domain name of domestic sites.<sup>103</sup> The government would have been limited to acting indirectly against foreign sites by requiring ISPs to block access to the infringing sites, credit card companies to suspend processing their transactions, and ad networks to suspend serving ads to them.<sup>104</sup> Additionally, the AG, through the U.S. IP Enforcement Coordinator, could publish a list of all domain names which the courts found to be infringing on copyright-protected content.<sup>105</sup> One troublesome provision would have allowed the AG to publish a list of sites simply alleged to be dedicated to infringing activity, even without a court order.<sup>106</sup> The bill would have also immunized ISPs, credit card companies and ad networks if they decided to act against alleged infringers.<sup>107</sup>

### C. PROTECT IP Act of 2011

Senators Leahy, Hatch, and Chuck Grassley (R-Iowa) introduced the PROTECT IP bill into the Senate on May 12, 2011.<sup>108</sup> The Senate Judiciary Committee voted unanimously to approve the bill on May 26, 2011.<sup>109</sup> The PROTECT IP Act extends COICA by authorizing the DOJ to use forfeiture proceedings, “against the registrant or owner of a domain name that accesses a foreign infringing Internet site, or the foreign-registered domain name itself,” upon a showing that the site is directed at U.S. consumers and harms holders of U.S. IP.<sup>110</sup> The bill attempts to add some due process protection by requiring potential plaintiffs to make some attempt to identify a person or entity in connection with the infringement before proceeding

---

<sup>103</sup> Better Enforcement, *supra* note 2.

<sup>104</sup> *Id.*

<sup>105</sup> *Id.*

<sup>106</sup> *Id.*

<sup>107</sup> *Id.*

<sup>108</sup> PROTECT IP, *supra* note 102.

<sup>109</sup> *Senate Judiciary Committee Unanimously Approves Bipartisan Bill To Crack Down On Rogue Websites*, LEAHY SENATE (May 26, 2011), [http://leahy.senate.gov/press/press\\_releases/release/?id=3520A48A-559E-436A-BDE5-32F4CFC5D05C](http://leahy.senate.gov/press/press_releases/release/?id=3520A48A-559E-436A-BDE5-32F4CFC5D05C).

<sup>110</sup> *Id.*

against the domain name itself.<sup>111</sup> PROTECT IP tries to narrow the definition of a rogue website,<sup>112</sup> while broadening enforcement mechanisms.<sup>113</sup> The AG would now be able to seek court orders against “servers of sponsored links” and “information location tools” or search engines, in addition to the other entities already covered under COICA.<sup>114</sup> Rights holders would also be able to bring actions against rogue sites, but with remedies limited to eliminating the financial viability of the site, not blocking access.<sup>115</sup>

D. The House’s Response to PROTECT IP – SOPA and OPEN

Congressman Lamar Smith (R-Tex.) introduced the Stop Online Piracy Act or SOPA, H.R. 3261, to the House Judiciary Committee on October 26, 2011.<sup>116</sup> The House Judiciary Committee held a hearing on SOPA on November 16, 2011,<sup>117</sup> but the Committee did not vote on the bill because of the magnitude of public outcry against it.<sup>118</sup> Senator Wyden and Congressman Darrell Issa (R-Calif.) introduced a draft version of an alternative bill to the public on December 8, 2011.<sup>119</sup> The Online Protection and Enforcement of Digital Trade Act or OPEN would expand the United States International Trade Commission’s existing authority to enforce

---

<sup>111</sup> Abigail Phillips, *The “PROTECT IP” Act: COICA Redux*, ELECTRONIC FRONTIER FOUNDATION (May 12, 2011), <http://www.eff.org/deeplinks/2011/05/protect-ip-act-coica-redux> [hereinafter COICA Redux].

<sup>112</sup> A rogue website has no significant use other than engaging in, enabling, or facilitating intellectual property infringement. See definition section of PROTECT IP bill, 3.

<sup>113</sup> PROTECT IP, *supra* note 102.

<sup>114</sup> COICA Redux, *supra* note 111.

<sup>115</sup> PROTECT IP, *supra* note 102.

<sup>116</sup> Declan McCullagh, *How SOPA would affect you: FAQ*, CNET NEWS (Dec. 21, 2011), [http://news.cnet.com/8301-31921\\_3-57329001-281/how-sopa-would-affect-you-faq/](http://news.cnet.com/8301-31921_3-57329001-281/how-sopa-would-affect-you-faq/).

<sup>117</sup> Lamar Smith, Chairman, Judiciary Committee, Statement at Hearing on H.R. 3261, the “Stop Online Piracy Act” (Nov. 16, 2011), available at <http://judiciary.house.gov/news/Statement%20HR%203261.html> [hereinafter SOPA].

<sup>118</sup> Steve Blank, *SOPA Is a Symbol of the Movie Industry's Failure to Innovate*, THE ATLANTIC (Jan. 6, 2012), <http://www.theatlantic.com/business/archive/2012/01/sopa-is-a-symbol-of-the-movie-industrys-failure-to-innovate/250967/>.

<sup>119</sup> Press Release, Wyden-Issa Release Draft Digital Trade Legislation, UNITED STATES SENATOR RON WYDEN (Dec. 8, 2011), <http://wyden.senate.gov/newsroom/press/release/?id=76dc4001-9cb8-42be-9c39-ebdc748162fc> [hereinafter Issa Draft].

copyright and trademark infringement as it currently applies to include websites.<sup>120</sup> Senator Wyden introduced OPEN in the Senate on December 17, 2011.<sup>121</sup>

A massive Internet campaign against SOPA and PROTECT IP – nicknamed “Blackout Day” – consisted of thousands of websites, including Google and other technology giants, causing their websites to go at least partially dark on January 18, 2012.<sup>122</sup> As a result, voting on PROTECT IP, scheduled for later that month,<sup>123</sup> was postponed so proponents and critics could work to resolve “legitimate issues” raised by the protest.<sup>124</sup> That same week, Congressman Smith followed suit and withdrew SOPA, vowing to redraft it.<sup>125</sup> Congressman Issa took advantage of the backlash against SOPA and PROTECT IP and officially introduced OPEN to the House on January 18, 2012.<sup>126</sup> Currently, the Senate version is in the Finance Committee, and the House bill is in the Judiciary Committee.<sup>127</sup>

## VI. THE DEBATE

Generally, critics of ICE and DOJ domain name seizures argue that the seizures and proposed legislation are overbroad, thereby increasing the risk of violating site owners’ due process and First Amendment rights; ineffective and wasteful; potentially harmful to the DNS;

---

<sup>120</sup> *Id.*

<sup>121</sup> Wikipedia entry for *Online Protection and Enforcement of Digital Trade Act*, [http://en.wikipedia.org/wiki/Online\\_Protection\\_and\\_Enforcement\\_of\\_Digital\\_Trade\\_Act](http://en.wikipedia.org/wiki/Online_Protection_and_Enforcement_of_Digital_Trade_Act) [hereinafter OPEN].

<sup>122</sup> *SOPA sent back to the drawing board in wake of Internet protests* (January 20, 2012), <http://latimesblogs.latimes.com/technology/2012/01/sopa-bill-sent-back-to-the-drawing-board-in-wake-of-internet-protests.html> [hereinafter Drawing Board]; *see also SOPA/PIPA Blackout By the Numbers* (January 19, 2012), <http://idealab.talkingpointsmemo.com/2012/01/sopapipa-blackout-by-the-numbers.php> [hereinafter Blackout].

<sup>123</sup> Declan McCullagh, *Senate will vote next month on Protect IP copyright bill*, CNET NEWS (Dec. 19, 2011), [http://news.cnet.com/8301-31921\\_3-57329001-281/how-sopa-would-affect-you-faq/](http://news.cnet.com/8301-31921_3-57329001-281/how-sopa-would-affect-you-faq/).

<sup>124</sup> PIPA anti-piracy bill vote postponed in Senate (January 20, 2012), <http://latimesblogs.latimes.com/technology/2012/01/pipa-anti-piracy-bill-vote-postponed-senate.html> [hereinafter, Postponed].

<sup>125</sup> Drawing Board, *supra* note 122.

<sup>126</sup> Issa Unveils Crowdsourced Sections of the OPEN Act (February 6, 2012), [http://issa.house.gov/index.php?option=com\\_content&view=article&id=957%3Aissa-unveils-crowdsourced-sections-of-the-open-act-&catid=63%3A2011-press-releases&Itemid=1](http://issa.house.gov/index.php?option=com_content&view=article&id=957%3Aissa-unveils-crowdsourced-sections-of-the-open-act-&catid=63%3A2011-press-releases&Itemid=1) [hereinafter, Crowdsourced].

<sup>127</sup> OPEN, *supra* note 121.

and likely tools to aid oppressive governments in censoring their citizens.<sup>128</sup> As for providing oppressive regimes with additional means to censor their people,<sup>129</sup> the possibility that someone might abuse a law does not mean the law should not be enacted. The other critiques will be addressed below.

A. The Proposed Legislation and ICE Seizures Are Overbroad and May Curtail Freedom of Speech and Due Process Rights.

Detractors point to questionable domain name seizures conducted by the DOJ as a foreshadowing of the Orwellian world to come if SOPA or PROTECT IP becomes law.<sup>130</sup> In “Operation Protect Our Children” – 84,000 lower-level domains were disrupted when the DOJ seized the TLD, mooo.com, for trafficking in child porn.<sup>131</sup> The DOJ then plastered a notice on each seized site to the effect that the site was shut down for trafficking in child pornography.<sup>132</sup>

---

<sup>128</sup> See Larry Downes, *Leahy’s Protect IP bill even worse than COICA*, CNET NEWS (May 12, 2011), [http://news.cnet.com/8301-13578\\_3-20062419-38.html#ixzz1MYFuCAYQ](http://news.cnet.com/8301-13578_3-20062419-38.html#ixzz1MYFuCAYQ); see Corynne McSherry, *U.S. Government Seizes 82 Websites: A Glimpse at the Draconian Future of Copyright Enforcement?*, ELECTRONIC FRONTIER FOUNDATION (Nov. 29, 2010), <http://www.eff.org/deeplinks/2010/11/us-government-seizes-82-websites-draconian-future> [hereinafter *Draconian Future*].

<sup>129</sup> Better Enforcement, *supra* note 2; EFF Open Letter, *infra* note 173.

<sup>130</sup> *Draconian Future*, *supra* note 129; see Letter from Kathryn Kleiman, Director of Policy for the Public Interest Registry, to Senate Judiciary Committee (Nov. 5, 2010) (*available at* [http://www.eff.org/files/filenode/coica\\_files/COICA%20Blocking%20Breaks%20DNSSEC%20-%20ORG%20Memo.pdf](http://www.eff.org/files/filenode/coica_files/COICA%20Blocking%20Breaks%20DNSSEC%20-%20ORG%20Memo.pdf)); see Letter from Law Professors’ Letter in Opposition to S. 3804 (Combating Online Infringements and Counterfeits Act), to Senate Judiciary Committee (*available at* [http://www.eff.org/files/filenode/coica\\_files/Professors%27%20Letter%20re%20COICA%20and%20Signatories.pdf](http://www.eff.org/files/filenode/coica_files/Professors%27%20Letter%20re%20COICA%20and%20Signatories.pdf)); see Letter from Markham C. Erikson, Partner Holch & Erickson LLP, Executive Director NetCoalition, to Chairman Patrick Leahy, Senate Judiciary Committee (Nov. 15, 2010) (*available at* [http://www.eff.org/files/filenode/coica\\_files/NetCoalition%20-%20Letter%20RE%20S3804%20COICA%2011.15.10.pdf](http://www.eff.org/files/filenode/coica_files/NetCoalition%20-%20Letter%20RE%20S3804%20COICA%2011.15.10.pdf)); see Letter from human rights organizations, to Chairman Patrick J. Leahy (Oct. 26, 2012) (*available at* [http://www.eff.org/files/filenode/coica\\_files/COICA\\_human\\_rights\\_letter.pdf](http://www.eff.org/files/filenode/coica_files/COICA_human_rights_letter.pdf)); see Edward Wyatt, *Lines Drawn on Antipiracy Bills*, N.Y. Times, Dec. 15, 2011, at B1, *available at* [http://www.nytimes.com/2011/12/15/technology/lines-are-drawn-on-legislation-against-internet-piracy.html?\\_r=3&sq=counterfeit&st=cse&sc=3&pagewanted=all](http://www.nytimes.com/2011/12/15/technology/lines-are-drawn-on-legislation-against-internet-piracy.html?_r=3&sq=counterfeit&st=cse&sc=3&pagewanted=all).

<sup>131</sup> *Draconian Future*, *supra* note 129; Nate Anderson, *Why the US needs to blacklist, censor pirate websites*, ARSTECHNICA (Apr. 1, 2011), <http://arstechnica.com/tech-policy/news/2011/04/why-the-us-needs-to-censor-pirate-websites.ars>; Nate Anderson, *Silicon Valley Congresswoman: Web seizures trample due process (and break the law)*, ARSTECHNICA (Mar. 14, 2011), <http://arstechnica.com/tech-policy/news/2011/03/ars-interviews-rep-zoe-lofgren.ars>.

<sup>132</sup> The message stated, “[a]dvertisement, distribution, transportation, receipt, and possession of child pornography constitute federal crimes that carry penalties for first time offenders of up to 30 years in federal prison, a \$250,000 fine, forfeiture and restitution.” See Ernesto, *U.S. Government Shuts Down 84,000 Websites ‘By Mistake’*, TORRENT



The government did not have to prove that all parts of the mooo.com domain name contained illegal material; they simply seized the TLD.<sup>133</sup> The DOJ started correcting its mistake within days, but being associated with child pornography most certainly already did some damage.

Supporters of government domain name seizures argue that the risks of error involved in seizing domain names are no higher than those involved in the seizure of personal property.<sup>134</sup> Critics counter that a domain name is more than personal property; it is the way other people, computers or search engines find a site.<sup>135</sup> It can also be a critical marketing and branding tool with substantial monetary value.<sup>136</sup> Critics claim that when a domain name is seized, the content gets locked away until a new domain is created.<sup>137</sup> However, that statement is not entirely factual because upon seizure, “the content and servers are still available to the owner, the site can still be accessed through the IP address, and it is relatively easy for the owner to acquire a new domain name – something many of those affected did within hours of having their domains seized.”<sup>138</sup> As for monetary value, the government routinely seizes valuable assets associated with criminal activity. Forfeiture of domain names is subject to the same considerations that justify no pre-seizure notice and hearing for personal property.<sup>139</sup> However, because websites contain potentially protected speech, they might need additional safeguards.

---

FREAK BLOG (Feb. 16, 2011), <http://torrentfreak.com/u-s-government-shuts-down-84000-websites-by-mistake-110216/> [hereinafter 84,000 Websites].

<sup>133</sup> Better Enforcement, *supra* note 2.

<sup>134</sup> Feds Seize, *supra* note 39.

<sup>135</sup> Makarewicz, *supra* note 79.

<sup>136</sup> *Id.*

<sup>137</sup> Feds Seize, *supra* note 39.

<sup>138</sup> *Id.*

<sup>139</sup> *Id.* (citing *Calero-Toledo v. Pearson Yacht Leasing Co.*, 416 U.S. 663, 678 (1974) citing *Fuentes v. Shevin*, 407 U.S. 67, 91 (1972), (“[I]n limited circumstances, immediate seizure of a property interest, without an opportunity for prior hearing, is constitutionally permissible. Such circumstances are those in which ‘the seizure has been directly necessary to secure an important governmental or general public interest. Second, there has been a special need for very prompt action. Third, the State has kept strict control over its monopoly of legitimate force: the person initiating the seizure has been a government official responsible for determining, under the standards of a narrowly drawn statute, that it was necessary and justified in the particular instance.’”).

1. Due Process Requires at Least a Prompt Post-Seizure Opportunity to Be Heard.

Even if the government is not automatically required to give pre-seizure notice, they must provide an immediate and meaningful opportunity for the domain name owner to be heard post-seizure.<sup>140</sup> Operation In Our Sites has not provided any such immediate hearing.<sup>141</sup> In Fact, weeks after Operation 2.0, site owners were still waiting to learn why their sites were seized,<sup>142</sup> and as late as April 2011, months after the first four seizure operations, this author could locate only one complaint seeking forfeiture, and it was filed months after the relevant seizure.<sup>143</sup>

Critics argue that even a prompt post-seizure hearing might be insufficient to truly compensate a domain name owner's loss caused by an erroneous seizure because an erroneous seizure may work to shut down a website indefinitely.<sup>144</sup> Unlike when the government seizes personal property, even if a domain is later restored, users who encountered ICE's seizure message at that domain will probably never return to the site.<sup>145</sup> While it seems reasonable to assume that some users would respond in this manner, this author is unconvinced that a significant number of users would respond in this manner. Users are probably just as likely to try to access the site repeatedly or conduct minimal research to find out why they are seeing the government's warning.

---

<sup>140</sup> Feds Seize, *supra* note 39, quoting *Heller v. New York*, 413 US 483, 489 (1973); *see also* Makarewicz, *supra* note 79.

<sup>141</sup> *Id.*

<sup>142</sup> Makarewicz, *supra* note 79.

<sup>143</sup> TVShack Complaint at 15, *supra* note 53.

<sup>144</sup> Makarewicz, *supra* note 79.

<sup>145</sup> *Id.*

2. While the Government's Initial Seizures Might Have Been Valid, Administrative Delay May Be Having the Effect of Improperly Censoring Protected Speech.

Since some of the seized domain names contain protected speech, the seizures must also comply with the freedom of speech provisions of the First Amendment.<sup>146</sup> Generally, the government must provide prior notice and an opportunity to be heard before it restrains “potentially protected speech, with the intent to take material out of circulation.”<sup>147</sup> Critics of the seizures contend that seizing an entire domain has the hallmarks of a prior restraint because in doing so, the government is indiscriminately taking both infringing and non-infringing material out of circulation.<sup>148</sup> But, improper censorship does not foreclose all seizures concerning speech.<sup>149</sup> It only requires that the government provide procedural safeguards to protect against the abridgment of speech rights,<sup>150</sup> namely, a valid warrant particularly describing the “things to be seized” and a judicial determination following an adversarial proceeding.<sup>151</sup>

Both Congresswoman Zoe Lofgren and Senator Wyden claim the warrants ICE obtained were invalid because they were merely rubber-stamped by magistrate judges.<sup>152</sup> On the contrary, the government seems to have met the warrant requirement as seizures are in most cases only authorized and made pursuant to valid, specific warrants issued by a neutral, impartial judge.<sup>153</sup> However, this author believes the government has failed to provide appropriate judicial

---

<sup>146</sup> *Id.*

<sup>147</sup> *Feds Seize*, *supra* note 39. (“*In Quantity of Copies of Books v. Kansas*, 378 US 205, 213 (1964), the Court reiterated its warning that “if seizure of books precedes an adversary determination of their obscenity, there is danger of abridgment of the right of the public in a free society to unobstructed circulation of nonobscene books.”).

<sup>148</sup> Makarewicz, *supra* note 79.

<sup>149</sup> *Id.*; *Magic Words*, *supra* note 37; *see also* *Feds Seize*, *supra* note 39.

<sup>150</sup> *Stanford v. Texas*, 379 US 476, 485 (1965).

<sup>151</sup> *Magic Words*, *supra* note 37.

<sup>152</sup> *Lofgren, Wyden Question Response to Seizure Inquiries*, CONGRESSWOMAN ZOE LOFGREEN, [http://lofgren.house.gov/index.php?option=com\\_content&view=article&id=637&Itemid=130](http://lofgren.house.gov/index.php?option=com_content&view=article&id=637&Itemid=130) (last visited Mar. 27, 2012) [hereinafter *Lofgren Questions*].

<sup>153</sup> *Magic Words*, *supra* note 37 (quoting *Heller v. New York*, 413 U.S. 483, 489 (1973)).

safeguards. A judicial determination can occur post-seizure, but must be prompt to prevent administrative delay from becoming a form of censorship.<sup>154</sup> Although Internet users can theoretically access the content of the sites by using the sites' IP addresses, the government's delay in commencing judicial proceedings effectively amounts to censorship because most users will not be able to access the sites.<sup>155</sup> Websites are assigned domain names because they are easier for humans to remember than numerical IP addresses. Most people are unlikely to have ever known, much less remember, the IP addresses of seized websites.<sup>156</sup> This author contends that the government's habit of delaying forfeiture proceedings means they are most likely running afoul of due process and First Amendment requirements. The government needs to provide clear and prompt mechanisms for judicial proceedings, commencing immediately upon seizing domain names.

B. Domain Name Seizures Are Ineffective As Owners Can Easily Move Domains to Different Domain Names After Seizure; Seizures Are Therefore a Waste of Resources.

The Electronic Frontier Foundation ("EFF") argues that the seizures show why this kind of enforcement is ineffective as seized sites were available at other domain names within mere hours.<sup>157</sup> Furthermore, third parties are creating alternative ways of providing access to seized domain name content. As an example, Mozilla<sup>158</sup> refused to remove an add-on from its website

---

<sup>154</sup> Makarewicz, *supra* note 79; *see also* Feds Seize, *supra* note 39.

<sup>155</sup> Makarewicz, *supra* note 79

<sup>156</sup> *Contra* Letter from Floyd Abrams, Partner at Cahill Gordon & Reindel LLP., to Chairman Patrick Leahy, Senate Judiciary Committee (Feb. 11, 2011) (*available at* <http://stage.dga.org/news/pr-images/2011/COICA-Letter-by-Floyd-Abrams.pdf>).

<sup>157</sup> COICA Redux, *supra* note 111; Ernesto, U.S. Seizes Sports Streaming Sites in "Super Bowl Crackdown", TORRENT FREAK BLOG (Feb. 2, 2011), <http://torrentfreak.com/u-s-seizes-sports-streaming-sites-in-super-bowl-crackdown-110202/> ("Rojadirecta is currently available on several alternative domains, including Rojadirecta.es., Channelsurfing.net is now available under Channelsurf.eu, Atdhe.net has moved to Atdhenet.tv and Ilemi.com transferred over to Ilemi.tv.").

<sup>158</sup> Mozilla is a non-profit organization dedicated to promoting openness by creating and sharing free software, like the Firefox webbrowser.

that ICE claimed circumvents the seizure order.<sup>159</sup> MafiaaFire Redirector 0.4b<sup>160</sup> was developed by MafiaaFire<sup>161</sup> and automatically redirects the user from the seized domain name to an alternate domain, outside the reach of the U.S. government.<sup>162</sup> Mozilla contends that removing the add-on is futile because even if they complied, the add-on would still be available on MafiaaFire's website.<sup>163</sup> Internet piracy will never be completely eradicated, but it can be dramatically reduced.<sup>164</sup> Minimizing it requires a mixture of tools, including education of consumers, a range of technical solutions, and of course, more aggressive enforcement of the legal rights of IPR holders.<sup>165</sup> Domain name seizures are but one tool of many to protect American ingenuity.

In judging effectiveness, one should look at whether the system can easily be defeated or circumvented without increasing inconvenience to the casual consumer of unlawful content.<sup>166</sup> Here, ICE's domain name seizures do appear to be easily circumvented simply by moving the site's contents to another server or locating it via the numerical IP address. Furthermore, third parties actively seek to circumvent the government's actions by providing alternative means of accessing seized domains.<sup>167</sup> COICA, PROTECT IP, and SOPA were implemented to plug some of these gaping loopholes by authorizing the government to enjoin third parties like credit card

---

<sup>159</sup> Harvey Anderson, *Homeland Security Request to Take Down MafiaaFire Add-on*, HJA'S BLOG, (May 5, 2011), <http://lockshot.wordpress.com/2011/05/05/homeland-security-request-to-take-down-mafiaafire-add-on/> [hereinafter Mozilla].

<sup>160</sup> For an explanation of how the add-on works, see *Frequently asked questions / wall of text!*, MAFIAA, <http://www.mafiaafire.com/wall-of-text.php> (last visited Mar. 27, 2012) [hereinafter Wall of Text].

<sup>161</sup> *Id.* MafiaaFire seems to have declared war on ICE and RIA and MPAA, in fact, Mafiaa stands for Music and Film Industry Association of America. The full name hints at the organizations goal of dissolving ICE and setting the music and film industry on fire. MafiaaFire is composed of anonymous members, probably located in Sweden.

<sup>162</sup> For details about the add-on, see *Add-Ons*, MOZILLA, <https://addons.mozilla.org/en-US/firefox/addon/mafiaafire-redirector/> (last visited Mar. 27, 2012).

<sup>163</sup> Ernesto, *Homeland Security Wants Mozilla to Pull "Domain Seizure" Add-On*, TORRENT FREAK BLOG (May 5, 2011), <http://torrentfreak.com/homeland-security-wants-mozilla-to-pull-domain-seizure-add-on-110505/> [hereinafter Mozilla Add-On]

<sup>164</sup> Better Enforcement, *supra* note 2; see also, Steal These, *supra* note 16 at I.

<sup>165</sup> Steal These, *supra* note 16 at I.

<sup>166</sup> *Id.* at 22.

<sup>167</sup> Mozilla Add-On, *supra* note 162.

companies from dealing with the seized domains, thereby making them commercially nonviable.<sup>168</sup> Additionally, since a large percentage of sites with infringing content are foreign websites, PROTECT IP and SOPA attempt to empower the DOJ to take specific action against them.<sup>169</sup> Of course, in exercising extraterritorial jurisdiction against foreign websites, the government runs the risk of impinging other countries' sovereignty. Congress must balance these competing interests when considering any legislation.

Opponents of domain name seizures also question whether this kind of action is the best use of DHS' resources. ICE, however, disputes the idea that they are wasting government resources by pursuing this seizure strategy.<sup>170</sup> According to ICE, only approximately 75 and 100 ICE agents worked on the first two rounds of Operation In Our Sites – about one-tenth of one percent of ICE-HSI agents.<sup>171</sup> Until we have evidence to the contrary, we must believe that domain name seizures are relatively economical.

C. Interference With the DNS Is Potentially Harmful to the Internet.

Other detractors are concerned about potential harm to the Internet infrastructure by fragmenting the DNS.<sup>172</sup> They predict that fragmentation will occur as domain names begin moving to alternative DNS's to avoid U.S. jurisdiction.<sup>173</sup> "This will cause numerous problems – including new network security issues, as a large percentage of the population moves to encrypted offshore DNS to escape the censoring effects of the procedures outlined in" the above-mentioned legislation.<sup>174</sup> However, interfering with the DNS to block access to websites or

---

<sup>168</sup> Leahy, *supra* note 2; PROTECT IP, *supra* note 102; *see also* SOPA, *supra* note 117.

<sup>169</sup> *See* PROTECT IP, *supra* note 102; *see also* SOPA, *supra* note 117.

<sup>170</sup> Chamber, *supra* note 50.

<sup>171</sup> *Id.*

<sup>172</sup> Mozilla, *supra* note 158; Peter Eckersley, *An Open Letter From Internet Engineers to the Senate Judiciary Committee*, ELECTRONIC FRONTIER FOUNDATION (Sept. 28, 2010) <http://www.eff.org/deeplinks/2010/09/open-letter> [hereinafter EFF open letter].

<sup>173</sup> *Id.*

<sup>174</sup> Draconian Future, *supra* note 128.

servers is not new – it has been used for blocking spam and protecting users from malware, for example, for many years.<sup>175</sup> Also, “many DNS resolvers routinely return different answers to users as part of a service, such as to provide parental filters, correct typos in URLs, or to provide search results in lieu of a basic “domain not found” error.”<sup>176</sup> This author believes unless ICE or DOJ go far beyond their mandates, the volume of seized domains is likely to remain relatively small. Furthermore, it seems illogical that a significant number of non-infringing websites are likely to proactively move their sites to servers outside the U.S.’s jurisdiction given the privacy and security considerations inherent in using foreign servers.<sup>177</sup> Therefore, domain name seizures will no more fragment the DNS than spam blockers.<sup>178</sup>

Critics also fear that domain name seizures will compromise the openness of the Internet. In fact, Mozilla refuses to remove the add-on partly because they share that belief.<sup>179</sup> But, the idea of a “free and open” Internet does not mean that every website has the right to exist.<sup>180</sup> Most people would probably agree that some websites should not be permitted to remain online, such as sites devoted to hosting child pornography or illegal scams.<sup>181</sup> The purpose of the ICE seizures and proposed legislation is not to shut down a personal website that accidentally links to a copyrighted image or websites that use material protected by fair use, but to shut down websites whose principal purpose is to engage in egregious infringement of IP.<sup>182</sup> A lot of the criticism of the legislation seems to have less to do with the law and more to do with pure

---

<sup>175</sup> Written Testimony Submitted for the Record of Daniel Castro Senior Analyst, Information Technology and Innovation Foundation (ITIF) on “Targeting Websites Dedicated To Stealing American Intellectual Property” before the Senate Committee on the Judiciary U.S. Senate (Feb. 12, 2011), *available at* <http://www.itif.org/files/2011-coica-testimony.pdf> [hereinafter Castro Testimony].

<sup>176</sup> *Id.*

<sup>177</sup> Daniel Castro, *No, COICA Will Not Break the Internet*, INNOVATION POLICY BLOG (Jan. 18, 2011), *available at* <http://www.innovationpolicy.org/no-coica-will-not-break-the-internet>.

<sup>178</sup> *Id.*

<sup>179</sup> David Carnoy, *ATDHE.NET MOVES AFTER HOMELAND SECURITY SEIZURE* (Feb. 4, 2011), [http://news.cnet.com/8301-17938\\_105-20030706-1.html?tag=mncol;txt](http://news.cnet.com/8301-17938_105-20030706-1.html?tag=mncol;txt).

<sup>180</sup> Castro Testimony, *supra* note 175.

<sup>181</sup> *Id.*

<sup>182</sup> *Id.*

ideology. namely, an opposition to any hint of an expansion of government authority and differing ideas of what an open Internet entails.<sup>183</sup> These are some of the issues the legislature needs to resolve when drafting new IP infringement legislation.

D. Domain Name Seizures Could Be One Useful Tool For Protecting IPR Owners.

The domain name seizure mechanism has some major flaws, but it is not completely without merit. Any enforcement legislation or protocol should be judged on its efficacy, intrusiveness, cost, and benefit.<sup>184</sup> As mentioned earlier, effectiveness is concerned with whether the system places a high enough burden on casual infringers attempting to circumvent the procedure.<sup>185</sup> Intrusiveness looks at whether the system imposes a more than *de minimis* burden on mainstream Internet users who are not engaged in unlawful activities and whether it violates expectations of privacy in any significant way.<sup>186</sup> If the system is excessively costly, especially with respect to its benefits, then it should be abandoned.<sup>187</sup> The system needs to make the enforcement of anti-piracy laws easier than before, without violating fundamental rights, such as self-expression and privacy.<sup>188</sup> “If a proposed system of enforcement seems to do well on most of these counts, it is likely worthy of a trial to determine its real-world utility.” Congress has the chance to craft IP enforcement legislation that meets all these factors.

## VII. CONCLUSION

The government has some compelling interests in pursuing domain name seizures – namely national security and economic stability. Although, domain name seizures are allowed under RICO, the scope is fairly limited. The domain name seizures currently being carried out

---

<sup>183</sup> *Id.*

<sup>184</sup> Steal These, *supra* note 16 at 22.

<sup>185</sup> *Id.*

<sup>186</sup> *Id.*

<sup>187</sup> *Id.*

<sup>188</sup> Steal These, *supra* note 16 at 22.



by ICE are ineffective because they can so easily be circumvented. A bill similar to PROTECT IP and SOPA would increase efficacy by giving the DOJ power to act against third parties, like credit card companies, thereby making subject domain names unprofitable.

As performed, ICE seizures are constitutionally questionable because of the delay in commencing judicial forfeiture proceedings. ICE must change this by providing and adhering to clear procedures for prompt judicial hearings following seizure. Congress should also be sure to include similar procedural safeguards in any proposed legislation to bring it into compliance with the Constitution. Neither the pending legislation nor the ongoing ICE seizures are perfect, but they are necessary steps in the government's efforts to protect American interests.