Berkeley Technology Law Journal

Volume 28
Issue 4 *Annual Review 2013*

Article 18

9-1-2013

Operation Seizing Our Sites: How the Federal Government is Taking Domain Names Without Prior Notice

Karen Kopel

Link to publisher version (DOI)
https://doi.org/10.15779/Z384Q3M

OPERATION SEIZING OUR SITES: HOW THE FEDERAL GOVERNMENT IS TAKING DOMAIN NAMES WITHOUT PRIOR NOTICE

Karen Kopel†

Imagine waking up one day to find that your website has been replaced with a banner posted by the federal government stating they have seized your domain name due to intellectual property crime violations:

Figure 1

That is exactly what happened to Andre Nasib's site, a popular hip-hop blog called Dajaz1.com. Without any prior notice or opportunity to defend the site, the Immigration and Customs Enforcement Office ("ICE") determined that Dajaz1.com was engaged in criminal copyright violations and was thus subject to forfeiture under 18 U.S.C. § 2323 due to four posted songs. As it turns out, those songs were sent to Dajaz1.com by the rights holders or their representatives in order for the influential site to promote the music, making

† J.D. Candidate, 2013, University of California, Berkeley School of Law.

it an authorized distribution. However, ICE agents relied on statements by representatives in the Recording Industry Association of America ("RIAA") in seizing the site and retaining it for over a year, waiting for the RIAA to get back to it with more evidence to proceed with forfeiture proceedings. Dajaz1 and its representatives incessantly tried to seek information from ICE and the prosecutors regarding the status of the site, but to no avail because the government had sealed the records. Despite seeking three secret *ex parte* extension orders from the court, the government never got the evidence it needed from the RIAA and eventually had to hand over Dajaz1.com back to its owner without an apology.[1]

Although this action of seizing a website may sound like a "digital Guantanamo,"[2] the process of seizing property (*in rem*) without any prior notice and without any opportunity for the party of interest to contest the original seizure (*ex parte*) has happened to thousands of domain names by the federal government under the intellectual property enforcement effort named Operation In Our Sites. Since its inception over two and a half years ago, Operation In Our Sites has seized 1,719 domain names of which over 690 have been forfeited,[3] ranging from websites selling allegedly counterfeit luxury goods, sports memorabilia, and pharmaceuticals, to websites that host copyrighted music, movies, TV shows, software, and websites that only link to this content.[4] Although this enforcement effort is grounded in noble policy reasons and backed by legitimate industry concerns,[5] the process that the National Intellectual Property Rights Coordination Center ("IPR

1. *See infra* Section II.C.1 (discussing the Dajaz1 case in detail).

2. Mike Masnick, *RIAA Tries To Downplay Its Role In The Feds' Unjustifiable Censorship of Dajaz1*, TECHDIRT (May 8, 2012, 8:14 AM), http://www.techdirt.com/articles/20120507/16073718821/riaa-tries-to-downplay-its-role-feds-unjustifiable-censorship-dajaz1.shtml (quoting Andrew Bridges, Dajaz1's attorney, in a statement following Dajaz1.com's return).

3. *See* News Release, U.S. Immigration and Customs Enforcement, Houston HIS Seizes 89 Websites Selling Counterfeit Goods (Dec. 20, 2012), *available at* https://www.ice.gov/news/releases/1212/121220houston.htm ("Under [Operation In Our Sites], 1,719 domain names have been seized since the operation began in June 2010. Since that time, the seizure banner has received more than 112 million individual views."); *see also infra* notes 30–36 and accompanying text (discussing the difference between seizure and forfeiture). Although this Note is current through December 2012, another seizure action took place in early 2013, resulting in a total of 2,061 websites seized under Operation In Our Sites. *See* News Release, U.S. Immigration and Customs Enforcement, ICE, CBP, USPIS Seize More Than $13.6 Million In Fake NFL Merchandise During 'Operation Red Zone' (Jan. 31, 2013), *available at* https://www.ice.gov/news/releases/1301/130131neworleans.htm.

4. *See* IPR Press Release, *infra* note 64; *see also infra* note 102.

5. *See infra* Section I.B (discussing the various policy reasons taken into account in the Joint Strategic Plans, which laid out the increased intellectual property enforcement efforts undertaken by the Obama Administration).

Center"), ICE, and the Department of Justice ("DOJ") employ to seize these domains has raised red flags among members of Congress and the public in general.[6] The *ex parte in rem* forfeiture proceedings allow the government to seize a domain name without any prior notice to the website operator, essentially leaving them in the dark. ICE agents and DOJ attorneys only need to show probable cause that the website in question engaged in one of the enumerated intellectual property violations in order to obtain a seizure warrant from a judge. These warrants are then served on the domestic domain name registries that are required to redirect each domain to a page that displays a banner explaining that the site has been seized pursuant to federal law.[7] To date, only two sites have successfully challenged their seizures,[8] yet their struggles in regaining control of their domain names have brought to light the lack of process and transparency that Operation In Our Sites affords those affected.

This Note will discuss Operation In Our Sites, which is part of a much broader intellectual property enforcement effort undertaken by the Obama Administration to combat all kinds of intellectual property violations. Part I discusses the background of the enforcement effort, focusing on the operation's authority granted by the Prioritizing Resources and Organization for Intellectual Property Act of 2008 ("Pro IP Act"), the policy reasons for increased intellectual property enforcement, and what Operation In Our Sites has been doing on the ground. Part II identifies the issues surrounding Operation In Our Sites, specifically addressing possible Due Process and First Amendment problems, along with other legal issues. It also provides an in-depth look at *Dajaz1* and *Rojadirecta*, the only two cases where website seizures were successfully challenged. The Note concludes with a discussion of the reality of the situation: although the process may not be perfect, it may be all we have. Rather than overhauling the entire system, the government

6. *See* Letter from Sen. Ron Wyden to John Morton, Director, U.S. Immigration and Customs Enforcement, and Eric Holder, Attorney General (Feb. 2, 2011), *available at* http://wyden.senate.gov/download/?id=103d177c-6f30-469b-aba8-8bbfdd4fd197 ("While I believe it important to combat copyright piracy, I grow concerned when the methods used may not be effective and could stifle constitutionally protected speech, job-creating innovation, and give license to foreign regimes to censor the Internet."); Letter from Rep. Zoe Lofgren to John Morton, Director, U.S. Immigration and Customs Enforcement (Apr. 7, 2011), *available at* http://lofgren.house.gov/images/stories/pdf/letter_to_morton_4-7.pdf; Letter from Rep. Zoe Lofgren, Rep. Jared Polis & Rep. Jason Chaffetz to Eric Holder, Attorney General, and Secretary Napolitano (Aug. 30, 2012), *available at* http://lofgren.house.gov/images/Letter_to_AG_Holder_083012.pdf.

7. *See supra* Figure 1; *infra* Section I.C.2 (describing the process and requirements of seizing a domain name).

8. *See infra* Section II.C (discussing the cases of Dajaz1 and Rojadirecta in depth).

should improve the enforcement of Operation In Our Sites to afford those affected transparency; specifically, enforcement agencies should be required to follow the statutory mandates or else return the domain name immediately.

I. BACKGROUND ON OPERATION IN OUR SITES DOMAIN NAME SEIZURES

To understand the legal implications of Operation In Our Sites, it is first important to have a grasp for where the authority of this operation has come from and how it has been implemented. Part I first discusses how the domain name seizure authority is governed by the Pro IP Act's civil forfeiture provisions,[9] which grant the federal government the power to first seize and then forfeit property that is used to facilitate one of the enumerated intellectual property violations.[10] The Act also created the position of the Intellectual Property Enforcement Coordinator ("IPEC") to coordinate enforcement efforts across the federal government and develop a plan to combat infringement.[11] Next, a discussion of the policy reasons behind the stronger enforcement effort and how the IPEC incorporated those reasons into her plan illuminates why such actions have been undertaken. The last Section of Part I discusses how Operation In Our Sites is working on the ground by identifying the actors involved, the process of seizing and forfeiting a domain name, and the timeline of seizure actions undertaken pursuant to the operation.

A. AUTHORITY: PRO IP ACT OF 2008

Operation In Our Sites is part of a much broader enforcement effort undertaken by the Obama Administration pursuant to the authority of the Pro IP Act.[12] Senate Judiciary Committee Chairman Patrick Leahy introduced the bill for the Pro IP Act, which President Bush signed into law on October 13, 2008.[13] The primary purpose of the Pro IP Act is to improve intellectual

9. *See* 18 U.S.C. § 2323(a) (2006).

10. *See* discussion *infra* Section I.C.2 (explaining how seizure and forfeiture are different and how the federal government must proceed in both instances).

11. *See* 15 U.S.C. § 8111 (2006).

12. Prioritizing Resources and Organization for Intellectual Property Act of 2008 ("Pro IP Act"), Pub. L. No. 110-403, 122 Stat. 4256 (codified at 18 U.S.C. § 2323 (2006)).

13. *See* Ray Dowd, *The Pro-IP Act of 2008: Copyright and Trademark Enforcement*, COPYRIGHT LITIGATION BLOG (Oct. 19, 2008), http://copyrightlitigation.blogspot.com/2008/10/pro-ip-act-of-2008-copyright-and.html.

property enforcement[14] by enhancing "civil and criminal penalties for intellectual property violations, [in order] to make commercial scale IP theft less profitable and easier to prosecute."[15] One way the Act increases intellectual property enforcement is by clearly and broadly applying seizure and forfeiture law to cases of intellectual property violations.[16] The Act also created roles for key intellectual property personnel in the executive branch to coordinate efforts across agencies and provide greater resources for those efforts.[17]

1. Civil Forfeiture Proceedings

The authority to conduct domain name seizures and forfeitures under Operation In Our Sites comes from the Pro IP Act's civil forfeiture provisions.[18] Inherited from English common law,[19] civil forfeiture is one of the oldest remedies and enforcement tools in the American legal system.[20]

14. *See* U.S. INTELLECTUAL PROPERTY ENFORCEMENT COORDINATOR, 2010 JOINT STRATEGIC PLAN ON INTELLECTUAL PROPERTY ENFORCEMENT 49 (JUNE 2010), *available at* http://www.whitehouse.gov/sites/default/files/omb/assets/intellectualproperty/intellectualproperty_strategic_plan.pdf [hereinafter JOINT STRATEGIC PLAN 2010]. ("[T[he term 'intellectual property enforcement' means 'matters relating to the enforcement of laws protecting copyrights, patents, trademarks, other forms of intellectual property, and trade secrets, both in the United States and abroad, including in particular matters relating to combating counterfeit and infringing goods.").

15. H.R. REP. No. 110-617, at 23 (2008).

16. *See* 18 U.S.C. § 2323. Civil forfeiture is not new to criminal copyright, however. Previously, copies of copyrighted material and the items used in their direct manufacture were subject to seizure. *See* 17 U.S.C. § 509(a) (repealed 2008).

17. H.R. REP. No. 110-617, at 23 ("[T]his Act will . . . institutionalize key IP enforcement within the Executive Office of the President . . . .").

18. *See* 18 U.S.C. § 2323; Brief of Amici Curiae Electronic Frontier Foundation, Center for Democracy and Technology, & Public Knowledge in Support of Puerto 80's Petition for Release of Seized Property at 1, Puerto 80 Projects, S.L.U. v. United States, No. 11-3983 (S.D.N.Y June 20, 2011) [hereinafter Brief of Amici Curiae] ("[T]he provisions purportedly authorize the government to seek in rem warrants for the seizure of property used to commit infringement.").

19. *See* 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, 276 (1995).

20. *See* J. W. Goldsmith, Jr.-Grant Co. v. United States, 254 U.S. 505, 508–11 (1921) (an early U.S. Supreme Court case affirming civil forfeiture of a car used to illegally transport fifty-eight gallons of distilled spirits for which taxes had not been paid). Originating from admiralty cases involving seizure of ships and other goods, civil forfeiture has evolved to cover tax evasion, bootleg liquor, and drug cases. *See* Ann Chaitovitz, Charisma Hampton, Kevin Rosenbaum, Aisha Salem, Tom Stoll & Albert Tramposch, *Responding to Online Piracy: Mapping the Legal and Policy Boundaries*, 20 COMMLAW CONSPECTUS 1, 4 (2011).

Civil forfeiture focuses on property, requiring *in rem* jurisdiction,[21] and is based on the legal fiction that the property itself can be found guilty.[22] In order to subject property to forfeiture, the government must show probable cause that the property in question was used in connection with, or is the proceed of, an illegal activity.[23] Since jurisdiction is asserted over the property itself, early Supreme Court jurisprudence established the notion that property could be seized regardless of the culpability of its owner.[24] This notion survives in civil forfeiture law today.[25]

---

21. *See* Lieske, *supra* note 19, at 271 (defining *in rem* jurisdiction required for civil forfeiture as "jurisdiction against the thing"). The critical distinction between forfeiture statutes is whether it is civil or criminal because each has its own jurisdictional requirement. Whereas civil forfeiture claims assert jurisdiction *in rem* over the property, criminal forfeiture statutes require *in personam* jurisdiction, which is jurisdiction based on the person, and thus implicate constitutional rights before the property can be seized. *Id.* at 271. The Pro IP Act also contains a criminal forfeiture provision, but that is out of the scope of this Note. *See* 18 U.S.C. § 2323(b).

22. *See* Lieske, *supra* note 19, at 266–67 (explaining that by focusing the relevant inquiry on whether the property in question is innocent or guilty, the government can circumvent an individual's constitutional rights); *see also* Mike Masnick, *DOJ: This Case Has Nothing To Do With Puerto 80; Now Here Is Why Puerto 80 Is Guilty*, TECHDIRT (Aug. 30, 2011, 9:09 AM), http://www.techdirt.com/articles/20110829/13225415732/doj-this-case-has-nothing-to-do-with-puerto-80-now-here-is-why-puerto-80-is-guilty.shtml. Masnick explained the government's argument in its reply to Puerto 80's motion to dismiss Rojadirecta's forfeiture proceedings:

> Specifically, the government is claiming that its sole reason for trying to forfeit the domain (and for seizing it in the first place) is that "those domain names themselves facilitated the commission of a recognized crime." That is, it argues that Puerto 80 is wasting its time in suggesting that *Puerto 80* did not engage in criminal copyright infringement, because the government has not charged Puerto 80 with anything. It's just claiming that the domains themselves are property used to commit a crime, and therefore can be forfeited.

Mike Masnick, *More & Bigger Mistakes Discovered In Homeland Security's Domain Seizures*, TECHDIRT (Dec. 22, 2010, 9:56 AM), http://www.techdirt.com/articles/20101222/02112912376/more-bigger-mistakes-discovered-homeland-securitys-domain-seizures.shtml

23. *See* Lieske, *supra* note 19, at 271 (arguing that probable cause is a low threshold for the government to meet).

24. *See id.* at 276–78 (discussing two early Supreme Court admiralty cases involving the seizure of ships due to the illicit conduct of individuals other than the ship's owner). "The Court reasoned that the culpability of the owner of the ship was not relevant because '[t]he thing is here primarily considered as the offender, or rather the offence is attached primarily to the thing.' " *Id.* at 277 (quoting The Palmyra, 25 U.S. (12 Wheat.) 1, 14 (1827)).

25. *See, e.g.*, *infra* Section II.B (explaining that linking sites have been seized pursuant to Section 2323's civil forfeiture authority because they link to websites that host the allegedly infringing content and thus "facilitate" the commission of a crime, despite the fact that neither the sites nor their operators are liable for criminal copyright infringement); *see also* Government's Memorandum of Law In Opposition To The Motion By Claimant Puerto 80 Projects, S.L.U. To Dismiss The Verified Complaint at 3, United States v. The Following

The Pro IP Act added 18 U.S.C. § 2323, which provides for civil forfeiture of property that is used to facilitate, or is the proceed of, certain enumerated intellectual property crimes, including criminal copyright and trademark counterfeiting.[26] Section 2323 incorporates the civil forfeiture procedures of the Civil Asset Forfeiture Reform Act of 2000,[27] which follows the Federal Rules of Criminal Procedure's rules for obtaining a search warrant.[28] Federal agents submit a sworn affidavit to a neutral federal magistrate. If the magistrate finds there is probable cause that the property is connected to the commission of criminal copyright infringement or trademark counterfeiting, the magistrate issues a seizure warrant.[29] Only then does the government initiate forfeiture proceedings against the property.

In order to understand the process afforded to domain names under Operation In Our Sites, it is important to note the difference between seizure and forfeiture—two related but distinct concepts. *Temporarily* taking custody of property related to a crime is seizure of that property.[30] The Fourth Amendment dictates that a lawful seizure of property be accompanied by a

---

Domain Names: rojadirecta.org, and rojadirecta.com, No. 11-4139 (S.D.N.Y. Aug. 26, 2011). In the *Rojadirecta* case, the Government explains that the action is against the domain name Rojadirecta, not against its operator Puerto 80:

> [T]he Government has neither charged Puerto 80 with a crime, nor has it filed a civil lawsuit against that company. Instead, and as the Complaint makes absolutely clear, the Government has brought a civil action against certain property—an *in rem* proceeding against two domain names that facilitated the commission of criminal copyright infringement and are thus subject to forfeiture pursuant to Section 2323(a)(I) of Title 18, United States Code.

Id.

26. 18 U.S.C. §§ 2323(a)(1)(B)–(C) (2006):

> The following property is subject to forfeiture . . . (B) [a]ny property used, or intended to be used, in any manner or part to commit or facilitate the commission of any offense referred to in subparagraph (A); (C) [a]ny property constituting or derived from any proceeds obtained directly or indirectly as a result of the commission of an offense referred to in subparagraph (A).

Id.

27. 18 U.S.C. § 2323(a)(2) (referencing 18 U.S.C. §§ 981–987 in mandating that "[t]he provisions of chapter 46 relating to civil forfeitures shall extend to any seizure or civil forfeiture under this section").

28. *See* 18 U.S.C. § 981(b)(2) ("Seizures pursuant to this section shall be made pursuant to a warrant obtained in the same manner as provided for a search warrant under the Federal Rules of Criminal Procedure . . . .").

29. *See infra* Section I.C.2 (discussing the process ICE and the IPR Center use in seizing a domain name pursuant to the authority of §§ 2323 and 981).

30. *See* Terry Hart, *Feds Seize Domain Names*, COPYHYPE (Dec. 6, 2010), http://www.copyhype.com/2010/12/feds-seize-domain-names/.

warrant issued upon probable cause that describes with particularity the thing to be seized.[31] Seizure in the online context differs from traditional seizure in that the government requires the domain name registry to redirect a suspected domain name to display a banner explaining that the site has been seized,[32] whereas traditionally seizure involves taking physical control over a tangible item.[33] Forfeiture, on the other hand, is the *permanent* involuntary divestiture of property to the government or other party without compensation due to breach or default of a legal obligation or commission of a crime.[34] Thus, property is forfeited to the U.S. government if it was used in the commission of a crime. Under Operation In Our Sites, the domain names are first temporarily seized pursuant to a warrant in order to

31. *See* U.S. Const. amend. IV. *But see* United States v. James Daniel Good Real Prop., 510 U.S. 43 (1993). The Court in *James Daniel* explains that the inquiry does not end at the Fourth Amendment:

> Though the Fourth Amendment places limits on the Government's power to seize property for purposes of forfeiture, it does not provide the sole measure of constitutional protection that must be afforded property owners in forfeiture proceedings. So even assuming that the Fourth Amendment were satisfied in this case, it remains for us to determine whether the seizure complied with our well-settled jurisprudence under the Due Process Clause.

Id. at 52.

32. *See supra* Figure 1.

33. *See* Brief of Amici Curiae, *supra* note 18, at 2. The Brief explains that seizure in the virtual context is a new application of the traditional seizure doctrine:

> The term 'seizure' is a misnomer in this context. One normally thinks of seizure in connection with the appropriation of real goods, such as counterfeit handbags or cars used in the commission of a crime. In these cases, however, the government has used section 2323 to require service providers to lock domain names pending transfer to the government, and to direct those domains to a web page announcing they have been seized.

Id. at 2; *see also infra* Section I.C.2 (discussing the process of seizing and forfeiting a domain name); *infra* notes 82–84 and accompanying text (summarizing the technical features of the domain name system in order to explain how seizure of a domain name works in comparison to seizure of a tangible, physical item).

34. Hart, *supra* note 30; *see* BLACK'S LAW DICTIONARY (9th ed. 2009) ("The loss of a right, privilege, or property because of a crime, breach of obligation, or neglect of duty."); *see also* Mike Masnick, *Breaking News: Feds Falsely Censor Popular Blog For Over A Year, Deny All Due Process, Hide All Details*, TECHDIRT (Dec. 8, 2011, 8:29 AM), http://www.techdirt.com/articles/20111208/08225217010/breaking-news-feds-falsely-censor-popular-blog-over-year-deny-all-due-process-hide-all-details.shtml (explaining that the difference between seizure and forfeiture is that the forfeiture process "allow[s] the government to keep the seized property and never have to give it back."); Lieske *supra* note 19, at 271 (discussing the difference between a criminal and civil forfeiture proceeding); *supra* note 21.

commence a civil forfeiture proceeding at a later date.[35] However, commentators have noted that this process of seizure in order to facilitate a forfeiture proceeding, in reality, seems like the sole purpose of the action under § 2323, rather than how the Act dictates the process.[36]

Although the Pro IP Act does not explicitly state that the civil forfeiture authority under § 2323 can be used to seize domain names involved in selling counterfeit goods and distributing pirated content, this is how the DOJ and ICE have interpreted their authority.[37] Neither the statute, the legislative history, nor any other document concerning the Act's creation discusses domain names or websites (used as the subject of the seizure and forfeiture).[38] Even commentators discussing the bill at the time of its development did not foresee the government interpreting the Act to apply to the online context. And no one anticipated that the Act would allow for the seizure of domain names.[39] However, this creative use of § 2323 is the legal basis for Operation In Our Sites.[40]

---

35. Hart, *supra* note 30 ("In short: property is *seized* to commence a civil forfeiture proceeding, and it is *forfeited* if it was used in the commission of a crime."); s*ee* Mike Masnick, *Tell The White House to Stop Illegally Seizing & Shutting Down Websites*, TECHDIRT (June 11, 2012, 8:21 AM), http://www.techdirt.com/articles/20120609/00050419257/tell-white-house-to-stop-illegally-seizing-shutting-down-websites.shtml ("ICE has been seizing (and in some cases forfeiting—which, in this context, means keeping, as 'seizure' is supposed to be a temporary process) website URLS.").

36. S*ee DOJ/FBI Seize Domain Names by Warrant*, TECH LAW JOURNAL (Aug. 21, 2012), *available at* http://www.techlawjournal.com/topstories/2012/home.asp [hereinafter *DOJ/FBI Seize Domain Names*] ("Nevertheless, this action [of seizures to facilitate forfeiture] has the appearance, not of pre-trial seizure of property for the purposes of preservation of property pending likely forfeiture upon final conviction, but rather of seizure as the sole object and purpose of the action."); *see, e.g.*, *infra* Section II.C.1 (discussing Dajaz1 and how the government obtained three extensions, far surpassing the statutorily mandated timeline dictating how long the government has to initiate forfeiture proceeding if the seizure is contested).

37. *See* Brian T. Yeh, *Online Infringement and Counterfeiting: Legislation in the 112th Congress*, 1099 PLI/PAT 693, 704 (2012); *DOJ/FBI Seize Domain Names*, *supra* note 36 (discussing the "innovative way" that the DOJ and ICE have begun using civil forfeiture authority).

38. *See* Yeh, *supra* note 37; *DOJ/FBI Seize Domain Names*, *supra* note 36. "Domain names" do not exist in the discourse surrounding the Pro-IP Act's enactment:

> Section 2323 does not refer to forfeiture of domain names. Moreover, a word search of the House and Senate floor debates on passage of the PRO-IP Act discloses that the subject of domain name seizures or forfeitures did not come up. Hence, the DOJ is using a statute that the Congress did not foresee would apply to domain names to seize domain names.

DOJ/FBI Seize Domain Names, *supra* note 36.

39. *See* William Patry, *What Does It Mean To Be Pro-IP?*, THE PATRY COPYRIGHT BLOG (Dec. 10, 2007), http://williampatry.blogspot.co.uk/2007/12/what-does-it-mean-to-be-pro-

2. Intellectual Property Enforcement Coordinator and the Joint Strategic Plan

To carry out the increased intellectual property effort, the Pro IP Act also created the IPEC, a position in the executive branch.[41] The IPEC's role is to coordinate the efforts of multiple federal agencies charged with intellectual property enforcement.[42] Under the Act, the IPEC is responsible for chairing an intellectual property advisory committee, developing a Joint Strategic Plan against piracy and counterfeiting with the advisory committee, assisting agencies and departments in the implementation of the Joint Strategic Plan, facilitating policy guidelines to help coordination among various actors in the government with respect to enforcement, offering suggestions to the President and Congress on possible improvements in enforcement efforts, and carrying out any other function with respect to intellectual property enforcement as the President may require.[43] Nicknamed the "intellectual property czar," Victoria Espinel was appointed as the IPEC in December 2009 and is the only person to serve in that position thus far.[44] She believes that enforcing intellectual property law is key in keeping the United States a leader in the global arena for innovation and creative expression, protecting the American economy by securing jobs domestically and guaranteeing a market for exports abroad, and ensuring public safety and health by reducing the risk that counterfeit products can pose.[45]

---

ip.html (arguing against adoption of the civil forfeiture bill on the grounds that the capacity of this provision is huge considering forfeiture is usually targeted at large scale criminal drug actors, but more importantly failing to foresee its application to internet domain names); *see also* Masnick, *Tell The White*, *supra* note 35 (discussing how even famed intellectual scholar William Patry did not anticipate that the civil forfeiture provision would be used to seize domain names, rather it was thought to be used to seize tangible property).

40. *See* Masnick, *Tell The White*, *supra* note 35 (explaining that ICE and DOJ pointed to section 2323 as "legal cover" for its actions of seizing domain names under Operation In Our Sites).

41. *See* 15 U.S.C. § 8111 (2006) ("The President Shall appoint, by and with the advice and consent of the Senate, an Intellectual Property Enforcement Coordinator . . . to serve within the Executive Office of the President."); *see also* JOINT STRATEFIC PLAN 2010, *supra* note 14, at 49 (explaining that the Obama Administration put the IPEC within the Executive's Office of Management and Budget). It is helpful to note that the IPEC is a position within the Executive Branch, not an agency.

42. *See* Victoria Espinel, *About the Office of the U.S. Intellectual Property Enforcement Coordinator (IPEC)*, OFFICE OF MANAGEMENT AND BUDGET, http://www.whitehouse.gov/omb/intellectualproperty/ipec/ (last visited Mar. 30, 2013).

43. *See* 15 U.S.C. § 8111(b)(1).

44. *See* JOINT STRATEGIC PLAN 2010, supra note 14, at 49 ("President Barack Obama nominated Victoria A. Espinel as the first IPEC on September 25, 2009, and the Senate confirmed Espinel on December 4, 2009.").

45. *See* Espinel, *About the Office of the IPEC*, supra note 42.

Under the Pro IP Act,[46] the IPEC is in charge of creating and implementing a Joint Strategic Plan, which is a "framework for coordinating and assessing federal efforts to combat piracy and counterfeiting."[47] The first Joint Strategic Plan was submitted to Congress in June 2010, and substantially similar plans with reiterated policy goals were released in 2011 and 2012.[48] The IPEC worked with many offices, departments, and agencies in the federal government in formulating the plans, including the Office of Management and Budget, DOJ, Federal Bureau of Investigation ("FBI"), ICE, Customs and Border Protection ("CBP"), Department of Health and Human Services, U.S. Patent and Trademark Office ("USPTO"), the U.S. Copyright Office, and many others.[49]

Espinel also solicited public input in her formulation of the first Joint Strategic Plan.[50] Specifically, she asked for comments and detailed recommendations addressing "the costs to the U.S. economy resulting from intellectual property violations, and threats to public health and safety created by infringement . . . and . . . the objectives and content of the Joint Strategic

---

46. *See* 15 U.S.C. §§ 8111(b)(1)(B) and 8113(a) (2006).

47. H.R. REP. No. 110-617, at 28 (2008). The House Report describes what the Joint Strategic Plan ("JSP") will include:

> The JSP will include detailed information on the threats of piracy and counterfeiting to the United States economy and to public health and safety; outline the various roles and responsibilities that government agencies will have in tackling intellectual property enforcement efforts; provide priorities and goals that will guide IP enforcement efforts; provide an accounting of the resources that will be needed to carry out the plan; and provide performance measures to gauge the success of the JSP in curbing counterfeiting and piracy.

Id. Note, for clarification, that the House Report uses the term Intellectual Property Enforcement Representative, which was a previous iteration of the current IPEC position. *Id.*

48. *See generally* JOINT STRATEGIC PLAN 2010, *supra* note 14; U.S. INTELLECTUAL PROPERTY ENFORCEMENT COORDINATOR, 2011 JOINT STRATEGIC PLAN ON INTELLECTUAL PROPERTY ENFORCEMENT (June 2011), *available at* http://www.whitehouse.gov/sites/default/files/omb/IPEC/ipec_anniversary_report.pdf [hereinafter JOINT STRATEGIC PLAN 2011]; U.S. INTELLECTUAL PROPERTY ENFORCEMENT COORDINATOR, 2012 JOINT STRATEGIC PLAN ON INTELLECTUAL PROPERTY ENFORCEMENT (June 2012), *available at* http://www.whitehouse.gov/sites/default/files/omb/IPEC/ipec_two-year_anniversary_report.pdf [hereinafter JOINT STRATEGIC PLAN 2012]. The act requires the IPEC to submit the Joint Strategic Plan to the Committees on the Judiciary and the Committees on Appropriates of both the House and the Senate. *See* 15 U.S.C. § 8113(b).

49. JOINT STRATEGIC PLAN 2010, supra note 14, at 49.

50. See JOINT STRATEGIC PLAN 2010, *supra* note 14, at 1 ("To prepare this Joint Strategic Plan, my office worked closely across numerous Federal agencies and departments and with significant input from the public. We heard from a broad array of Americans and received more than 1,600 public comments with specific and creative suggestions.").

Plan and other specific recommendations for improving the Government's intellectual property enforcement efforts."[51] In their responses, various intellectual property public interest organizations such as Public Knowledge and the Electronic Frontier Foundation ("EFF") recommended that the IPEC, in its creation of the Joint Strategic Plan, focus only on the worst actors that cause the most public harm or act willfully, a higher standard than merely infringing.[52] These groups also emphasized that any enforcement action must be clearly weighed because bad social and economic outcomes could result if enforcement of private rights is taken too far.[53] Furthermore, the IPEC met with industry leaders on both sides of the intellectual property debate and incorporated their concerns into its plan.[54]

The result of these discussions is a Joint Strategic Plan that focuses on six categories of action items: "(1) leading by example; (2) increasing transparency; (3) ensuring efficiency and coordination; (4) enforcing our rights internationally; (5) securing our supply chain; and (6) building a data-driven Government."[55] The subsequent plans, although much shorter than the earlier plans, incorporate these concepts by explaining the significant progress the Administration has made in intellectual property enforcement by seizing numerous domain names, obtaining significant convictions, and encouraging voluntary actions by the private sector.[56] The IPEC has also

51. Coordination and Strategic Planning of the Federal Effort Against Intellectual Property Infringement: Request of the Intellectual Property Enforcement Coordinator for Public Comments Regarding the Joint Strategic Plan, 75 FED. REG. 35, 8137 (Feb. 23, 2010). However, some question whether the IPEC was as open-minded in soliciting public opinion as she appeared. *See* John Bergmayer, IPEC Asks Loaded Questions, But Public Can Respond, PUBLIC KNOWLEDGE, (Feb. 25, 2010), http://www.publicknowledge.org/node/2922 ("While I'm confident that public participation will give the office the information it needs to recommend a balanced approach to IP enforcement priorities, the leading questions and loaded words used in the Notice are a cause for concern.").

52. See Public Comment from Public Knowledge, Electronic Frontier Foundation, American Association of Law Libraries, Medical Library Association, Special Libraries Association, and U.S. PIRG, In the Matter of Coordination and Strategic Planning of the Federal Effort Against Intellectual Property Infringement: Request of the Intellectual Property Enforcement Coordinator For Public Comments Regarding the Joint Strategic Plan, at 6–8, *available at* https://www.eff.org/files/filenode/PK-EFF-et-al-JSP-comments.pdf.

53. *See id.* at 2–6.

54. *See* JOINT STRATEGIC PLAN 2010, *supra* note 14, at 49.

55. *Id.* at 7. See *id.* at 7–22 for a description of each of the six categories of enforcement strategy action items and what specifically each entails.

56. *See* JOINT STRATEGIC PLAN 2011, *supra* note 48, at 1; JOINT STRATEGIC PLAN 2012, *supra* note 48, at 1. The IPEC, Victoria Espinel, boasted:

> It has been two years since my office issued the Joint Strategic Plan on Intellectual Property Enforcement, which set forth thirty-three action

released two annual reports—in February 2011 and March 2012—detailing the progress of intellectual property enforcement that the Plan called for.[57] Specifically, the Annual Reports highlighted the steps the IPEC, along with the agency she works with, has taken to implement the plans.[58]

B. THE ESTABLISHMENT OF OPERATION IN OUR SITES

The 2010 Joint Strategic Plan developed by IPEC lays out numerous policy reasons for increasing intellectual property enforcement.[59] These policy reasons include "growth of the U.S. economy; creation of jobs for American workers and support for U.S. exports; promotion of innovation and security of America's competitive advantage in the global economy; protection of consumer trust and safety; national and economic security; and validation of rights as protected under our Constitution."[60] Most of these reasons are rooted in the concern that the United States will lose its global economic advantage if its intellectual property is not protected.[61]

> items organized under six overarching principles that contribute to protecting innovation, strengthening the economy, supporting American jobs, and promoting export in intellectual property-related sectors. I am pleased to share highlights of our success over the past two years.

JOINT STRATEGIC PLAN 2012, *supra* note 48, at 1.

57. *See* U.S. INTELLECTUAL PROPERTY ENFORCEMENT COORDINATOR, 2010 ANNUAL REPORT ON INTELLECTUAL PROPERTY ENFORCEMENT (Feb. 2011), *available at* http://www.whitehouse.gov/omb/intellectualproperty [hereinafter ANNUAL REPORT 2010]; U.S. INTELLECTUAL PROPERTY ENFORCEMENT COORDINATOR, 2011 ANNUAL REPORT ON INTELLECTUAL PROPERTY ENFORCEMENT (Mar. 2012), *available at* http://www.whitehouse.gov/omb/intellectualproperty [hereinafter ANNUAL REPORT 2011].

58. *See* ANNUAL REPORT 2010, *supra* note 57, at 1–2. Espinel explains the work the federal government has done since the implementation of the first Joint Strategic Plan:

> Since we issued the Strategy, the U.S. Government has been hard at work implementing the action items and taking concrete steps to improve enforcement. I want to highlight a few of our important steps . . . . In the Strategy, we committed to increase criminal enforcement. Among the major law enforcement actions: [ICE, DOJ, and the IPR Center] launched Operation In Our Sites and obtained court orders to seize the domain names of more than 90 infringing websites.

Id. at 1–2; *see also* ANNUAL REPORT 2011, *supra* note 57, at 1–3.

59. *See* JOINT STRATEGIC PLAN 2010, *supra* note 14, at 3–5.

60. *Id.* at 3–4.

61. *See id.* at 4–5. Explaining the United States' dominant role in the intellectual property sector:

> The U.S. is a global leader in developing new technologies in intellectual property-related industries. . . . [W]e lead the way in bringing new, life-changing pharmaceuticals and medical devices to consumers, developing environmentally-conscious technologies, creating innovative software products, building new communication networks and producing films,

In order to carry out the 2010 strategic plan for protecting intellectual property online, the Obama Administration established Operation In Our Sites. Because the Internet has facilitated the explosive growth of piracy and counterfeiting, which significantly impacts the U.S. economy, hampers consumer trust, and poses health and safety risks,[62] the Obama Administration prioritized and increased intellectual property enforcement.[63] Accordingly, in June 2010, the administration initiated Operation In Our Sites as a multi-agency program designed to investigate and combat sales of counterfeit goods and criminal copyright infringement committed over the Internet by seizing the domain names suspected of engaging in these illicit activities.[64] Operation In Our Sites is only one out of thirty-three intellectual property enforcement operations undertaken by the IPEC in the Joint Strategic Plans.[65]

C. OPERATION IN OUR SITES ON THE GROUND: WHAT HAS REALLY BEEN HAPPENING

To really understand Operation In Our Sites, it is important to understand what this operation is actually doing day-to-day. This Section discusses the actors carrying out the operation,[66] the statutorily mandated process for seizing and forfeiting a domain name, and the specific seizure actions that the government has carried out.[67]

> music and games craved by consumers throughout the World. However, our leadership in the development of creative and innovative products and services also makes us a global target for theft.

Id.

62. *Id.* at 3–4.

63. *See* Chaitovitz, *supra* note 20, at 2 ("In response to the challenges posed by online piracy and counterfeiting, the Obama Administration has made intellectual property protection and enforcement a high priority.").

64. *See* Press Release, National Intellectual Property Rights Coordination Center, Operation In Our Sites, *available at* www.iprcenter.gov/reports/fact-sheets/operation-in-our-sites/view [hereinafter IPR Press Release].

65. *See* ANNUAL REPORT 2010, supra note 57, at 33–57 (discussing the various programs that the IPEC has initiated for increased intellectual property enforcement across the entire federal government; the first Joint Strategic Plan introduced in 2010 included thirty-three specific actions intended to improve intellectual property enforcement by the federal government); *see also* Victoria Espinel, *Progress on the Intellectual Property Enforcement Strategy*, THE WHITE HOUSE BLOG (Feb. 7, 2011, 4:00 PM), http://www.whitehouse.gov/blog/2011/02/07/progress-intellectual-property-enforcement-strategy.

66. But note that this is not an exhaustive list as the inter-agency relationship the operation calls for is always expanding.

67. Although this list may seem long, it is important because it is difficult to find a comprehensive and thorough list of all the seizure actions in one place.

1. Who Is Involved?

In creating the IPEC, the Pro IP Act attempts to address a need to coordinate intellectual property enforcement efforts across all the federal agencies whose interests are implicated. Thus, different interagency partnerships are created to carry out over thirty action items specified in the Joint Strategic Plans.[68] For example, the IPR Center,[69] which ICE leads and manages,[70] coordinates the Operation In Our Sites effort across many federal agencies. Over the course of its existence, the IPR Center has grown to incorporate the expertise of twenty-one member agencies in an interagency partnership charged with sharing information, developing initiatives, coordinating enforcement actions, and conducting investigations related to intellectual property theft.[71] Member agencies include the FBI, CBP, the DOJ, the Food and Drug Administration, and the USPTO, along with international agencies such as INTERPOL.[72]

---

68. *See supra* note 65 and accompanying text.

69. *See generally* JOINT STRATEGIC PLAN 2010, *supra* note 14, at 28. The IPR Center was established in order:

> To more effectively counter the flood of infringing products, ICE established the IPR Center. The mission of the IPR Center is to address and combat predatory and unfair trade practices that threaten our economic stability and national security, restrict the competitiveness of U.S. industry in world markets, and place the public's health and safety at risk.

Id.

70. *See generally id.* ("ICE is a lead U.S. agency for the investigation of criminal intellectual property violations involving the illegal production, smuggling, and distribution of counterfeit and pirated products . . . . [It] seizes for forfeiture goods associated with these investigations, such as those that infringe on trademarks, trade names, and copyrights.").

71. *See* News Release, U.S. Immigration and Customs Enforcement, European Law Enforcement Agencies and Europol Seize 132 Domain Names Selling Counterfeit Merchandise in 'Project Cyber Monday 3' and 'Project Transatlantic Operations' (Nov. 26, 2012), *available at* http://www.ice.gov/news/releases/1211/121126washingtondc.htm ("[T]he IPR Center uses the expertise of its 21 member agencies to share information, develop initiatives, coordinate enforcement actions, and conduct investigations related to IP theft. Through this strategic interagency partnership, the IPR Center protects the public's health and safety, the U.S. economy and the war fighters.").

72. *See About Us*, NATIONAL INTELLECTUAL PROPERTY RIGHTS COORDINATION CENTER (last visited Jan. 22, 2013), http://www.iprcenter.gov/about-us. Also included are agencies within other governments including the Royal Canadian Mounted Police, the Mexican Revenue Service, and EUROPOL. *Id. See also* JOINT STRATEGIC PLAN 2011, *supra* note 14, at 1 ("[T]he following now have representatives at the [IPR Center]: four previously unrepresented Federal agencies, a foreign government, and for the first time, an international law enforcement body.").

2. The Process of Seizing and Forfeiting a Domain Name

Domain name seizures generally follow a set series of steps, informed by Chapter 46 of Title 18.[73] Before initiating a seizure, federal officers investigate the websites suspected of selling counterfeit goods or illegally distributing copyrighted material in the United States.[74] For counterfeit goods, ICE and the IPR Center purchase these goods through suspected websites and have them shipped to federal agents.[75] The goods generally have to cross the U.S. border because most of the suspected websites operate abroad.[76] Once the agents have received the goods, they contact the rights holders to confirm that the goods are infringing or otherwise illegal.[77] For copyrighted material, the ICE and the IPR Center investigate possible violations by downloading or streaming the content and then checking with the rights holder to confirm that the content is protected.[78] The ICE and IPR Center present the evidence obtained from these investigations to DOJ attorneys, who work alongside ICE and the IPR Center to determine whether there is enough evidence to obtain a seizure order for each site investigated.[79] A determination is then made whether the domain names are registered in the United States, even if the website is operated overseas.[80]

---

73. *See* 18 U.S.C. §§ 981(b)(2), 983 (2006) (setting out the procedure the government must follow in conducting civil forfeiture).

74. *See* Letter from John Morton, Director, U.S. Immigration and Customs Enforcement, to Rep. Zoe Lofgren (May 9, 2011), *available at* http://www.wyden.senate.gov/download/?id=598c62fd-47ad-4372-828e-7694b6821e3f ("Although ICE cannot discuss the ongoing investigations of any seized domain name or a matter in litigation, ICE conducted thorough independent investigations of each seized domain name prior to obtaining court-ordered seizure warrants.").

75. *See* Brian W. Brokate & Christina L. Winsor, *Developments In Anti-Counterfeiting Enforcement and Remedies—What's Working And What's Not?*, 1103 PLI/PAT 795, 827 (2012); *see, e.g.*, News Release, ICE, 'Operation Strike Out,' *infra* note 128 ("During the course of the operation, federal law enforcement agents made undercover purchases of sport jerseys from online retailers suspected of selling counterfeit goods.").

76. *See* Chaitovitz, *supra* note 20, at 12–13; s*ee, e.g.*, News Release, ICE, 'Operation Strike Out,' *infra* note 128 ("In most instances, the counterfeit goods were shipped directly into the United States from suppliers in other countries using international express mail.").

77. *See* Brokate & Winsor, *supra* note 75, at 827.

78. *See* Affidavit in Support of Application for Seizure Warrant at ¶¶ 8, 17, 28, United States v. The Following Domain Names: rojadirecta.org, and rojadirecta.com, No. 11-MAG-262 (S.D.N.Y. Jan. 31, 2011) [hereinafter Rojadirecta Affidavit]; Application and Affidavit for Seizure Warrant at ¶¶ 79–82, In re Seizure of The Following Domain Names: RapGodFathers.com, et al., No. 10-2822M (C.D. Cal. Nov. 17, 2010), *available at* http://s3.amazonaws.com/nytdocs/docs/543/543.pdf [hereinafter Dajaz1 Affidavit].

79. Several other factors are taken into consideration before a determination of whether the site should be seized is made, including: the popularity of the site; whether the website is commercial in nature and is profitable, such as sites that utilize advertisements and

The ICE and IPR Center present affidavits to a federal magistrate judge, who makes an independent probable cause determination.[81] If the judge concludes there is enough evidence of criminal copyright or trademark infringement, he or she grants a seizure order that is served on the domestic domain name registry,[82] not the website operator. Under the seizure order, the domain name registry must restrain and lock the domain name pending completion of the forfeiture proceeding, at which time the domain name's title, rights, and interests are transferred to the U.S. government.[83] The registry is required to redirect the domain name to a different IP address with its own web page. That web page displays a banner stating that the domain name for that website has been seized by the FBI, ICE, and IPR Center pursuant to a seizure warrant under the authority of 18 U.S.C. §§ 981 and 2323.[84] Although the banners differ slightly depending on the nature of the

sell subscriptions or merchandise; and whether the seizure of the domain name would have a substantial impact on piracy. *See* Yeh, *supra* note 37, at 704.

80. *See* 18 U.S.C. § 2323 (2006) (authority that only has jurisdiction over websites registered in the United States); Yeh, *supra* note 37, at 705 ("Only domain names registered within the United States and subject to ICE's jurisdiction may be seized."). *See generally supra* note 82 (noting that all ".com," ".net," and ".org" top-level domains ("TLDs") are managed by American registries); Chaitovitz, *supra* note 20, at 12–13 (noting that because most of these websites are operated in foreign countries and that there may not be any known assets in the United States, seizure of a domain name with U.S. registration is the only remedy available).

81. *See* Yeh, *supra* note 37, at 704 ("In order to issue the warrant, the [magistrate] judge must determine, by a standard of probable cause, that the domain name is being used in violation of federal criminal laws."). *See generally supra* text accompanying note 23.

82. *See generally* Jonathan Weinberg, *ICANN and the Problem of Legitimacy*, 50 DUKE L.J. 187, 194–98 (2000) (defining "registries" and explaining how Internet Protocol and the Domain Name System ("DNS") works). The Internet transfers data and information over numerical Internet Protocol addresses ("IP addresses") that are tied to a network of computers. *Id.* at 194–95. To access a particular website's data, an individual can type in that website's IP address; however, because IP addresses are long and complex series of numbers that are difficult to remember, the DNS was created to associate an IP address with a website's name. *Id.* at 195–96. When a user types in the name of the website, the DNS server corresponds the name to the IP address. *Id.* at 197. All domain names have a suffix, or top-level domain ("TLD"), such as ".com," ".net," and ".org" that identifies what type of website it is. *Id.* at 197–99. Registries are companies that manage a specific type of TLD. *Id.* at 202. For instance, all ".net," ".org," and ".com" TLDs are managed by registries located within the United States. *See* Chaitovitz, *supra* note 20, at 7.

83. *See* Chaitovitz, *supra* note 20, at 7; Brief of Amici Curiae, *supra* note 18, at 2–4 (discussing what seizure of a domain name really entails and how the term is odd in the context of an intangible item).

84. *See supra* Figure 1; Chaitovitz, *supra* note 20, at 7. It is important to note that the seizure of a domain name does not result in the blocking of a website, rather it leaves the IP address and the files associated with the IP address intact so visitors can still see the website by typing in the IP address instead of typing the domain name that has been seized. Chaitovitz, *supra* note 20, at 7–8.

site seized and the agencies involved, they usually contain a statement that willful copyright infringement[85] and intentionally and knowingly trafficking in counterfeit goods[86] are federal crimes that carry serious penalties.[87] Individuals who access a seized domain name will see the banner in place of the content that the website once displayed.[88]

Only then do individuals with an interest in the seized website have an opportunity to try to contest the seizure. The government is required to send written notice to the website operator within sixty days of seizing the domain name or to file a judicial forfeiture action against the property and provide notice of that action to interested parties.[89] The website owner is allowed to file a claim with the agency within the deadline set in the written notice of forfeiture.[90] Within ninety days of filing the claim, the government must file a complaint for forfeiture, include the property in a criminal indictment, or return the property pending the filing of a complaint.[91] During this hearing process to determine the validity of the affidavit supporting the seizure, the government carries the burden of proof to show that the information in the affidavit is correct.[92] If the website owner does not file a petition or claim before the set deadline, the domain name automatically becomes property of the U.S. government subject to the forfeiture provisions.[93] In April 2011, ICE launched a PSA announcement to help raise awareness of the cost of

85. *See* 17 U.S.C. § 506(a) (2006) (defining criminal copyright infringement); 18 U.S.C. §§ 2319(a)–(d) (2006) (detailing the punishments for criminal copyright infringement). Willful copyright infringement is a federal crime that carries penalties for first time offenders of up to five years in federal prison, a $250,000 fine, forfeiture, and restitution. *See* Kravets, *infra* note 221 for this language on the banner.

86. *See* 18 U.S.C. § 2320 (2006). Intentionally and knowingly trafficking in counterfeit goods is a federal crime that carries penalties for first time offenders of up to ten years in federal prison, a $2,000,000 fine, forfeiture and restitution. 18 U.S.C. § 2320(b)(1)(A).

87. Seizure banner statements are generally very vague and do not clarify if the person visiting the site would be liable for either of these types of violations or if it is the website itself that has committed the crime.

88. *See* News Release, ICE, Houston HIS Seizes, *supra* note 3 ("Under [Operation In Our Sites], 1,719 domain names have been seized since the operation began in June 2010. Since that time, the seizure banner has received more than 112 million individual views.").

89. 18 U.S.C. §§ 983(a)(1)(A)(i)–(ii) (2006).

90. *Id.* § 983(a)(2).

91. *Id.* § 983(a)(3).

92. *Id.* § 983(c)(1).

93. *See* News Release, ICE, Houston HIS Seizes, *supra* note 3 ("If no petitions or claims are filed, the domain names become the property of the U.S. government."); *see also* Masnick, *Breaking News*, *supra* note 34 (discussing the process of seizure and forfeiture and explaining the timeline between the two).

intellectual property theft, which it placed on forfeited websites in lieu of the seizure banner after the website had been forfeited.[94]

Director Morton of ICE explains there are other avenues afforded to individuals who wish to obtain due process and regain their domain name:

> Under existing federal law, the website owner may also choose to demand return of the property through the law enforcement agency itself, by writing a letter to ICE. If ICE does not return the website within 15 days, the owner can petition the U.S. District Court in which the seizure warrant was issued or executed. Further, if the website owner determines he or she does not wish to pursue either of these avenues of due process, a challenge may be filed directly with the law enforcement agency conducting [a] forfeiture action under administrative processes.[95]

However, publicized events and public commentary have brought to light the difficulty website owners face in challenging their property seizure in court or through the agencies themselves.[96] Specifically, opponents have pointed out that despite ICE's claims about how rarely people challenge the seizure of their sites (and thus justifying the large number of sites that have automatically been forfeited), many website operators have indeed contacted agents in an effort to regain their domain names.[97] However, they claim that the government uses intimidation tactics by threatening to file charges or stalling their requests in order to persuade these parties not to file the claims.[98]

---

94. *See* News Release, U.S. Immigration and Customs Enforcement, New Public Service Announcement Launched to Raise Intellectual Property Theft Awareness 65 Seized Websites Now Feature PSA (Apr. 26, 2011), *available at* https://www.ice.gov/news/releases/1104/110426washingtondc.htm.

95. *See Promoting Investment and Protecting Commerce Online: Legitimate Sites v. Parasites, Part II: Hearings Before the H. Subcomm. on Intellectual Property, Competition, and the Internet*, 112th Cong. 117 (2011) (statement of John Morton, Director, ICE).

96. *See infra* Section II.C (discussing the only two examples of sites successfully challenging their seizure and forfeiture of their sites: the Dajaz1 and Rojadirecta cases).

97. *See* Masnick, *Breaking News*, *supra* note 34 ("[T]he government began stalling like mad when contacted by representatives for domain holders seeking to get their domains back. ICE even flat out lied to the public, stating that no one was challenging the seizures, when it *knew* full well that some sites were, in fact, challenging.").

98. *See id.* ("If that doesn't happen, the government can effectively just keep the property, so it tends to rely on intimidation and threats towards anyone who indicates plans to ask for their property back (usually in the form of threatening to file charges).").

3. Timeline of the Specific Phases

Since its inception in late June 2010, Operation In Our Sites has seized 1,719 domain names[99] allegedly involved in criminal copyright or counterfeit goods violations.[100] Many types of domain names have been targeted, including linking sites,[101] websites engaged in direct copyright infringement, and websites selling counterfeit goods, including sports items, luxury goods, and pharmaceuticals.[102] There have been ten reported phases and numerous subsequent seizure actions associated with Operation In Our Sites, which are described below.[103] An overview of the specific actions taken under this operation is helpful in understanding the scope of this enforcement action, as it is difficult to find one cohesive list detailing all the seizures.[104]

June 30, 2010, marked the first phase of Operation In Our Sites with the seizure of nine domain names and confiscation of $84,000.[105] The IPR

99. *See* News Release, ICE, Houston HIS Seizes, *supra* note 3 (stating Operation In Our Sites has seized 1,719 domain names up through December 2012, of which over 690 domains have been forfeited to the U.S. government).

100. There is some discrepancy about the exact number of sites that have been seized by Operation In Our Sites as reports from IPEC, ICE, and IPR Center sometimes have varying accounts of the total amount of sites seized per phase and whether a seizure of a domain name was pursuant to Operation In Our Sites or some other Initiative pursued by IPEC.

101. A "linking" site is a type of website that provides access, or "links," to other websites where pirated content is hosted. News Release, U.S. Immigration and Customs Enforcement, New York Investigators Seize 10 Websites That Illegally Streamed Copyrighted Sporting and Pay-per-view Events (Feb. 2, 2011), *available at* http://www.ice.gov/news/releases/1102/110202newyork.htm. These types of sites are popular because they allow visitors to easily browse content and locate streams or downloads that is usually very difficult to find with regular search engines. *Id.*

102. *See* IPR Press Release, *supra* note 64 ("Operation In Our Sites specifically targets websites and their operators that distribute counterfeit and pirated items over the Internet, including counterfeit pharmaceuticals and pirated movies, television shows, music, software, electronics, and other merchandise as well as products that threaten public health and safety.").

103. Since the beginning of 2012, ICE press releases and IPEC's IPS Spotlights has not designated an action as a "version" as previously done in 2010 and 2011, making the different phases of Operation In Our Sites more difficult to track. However, for each action in 2012, some authority from a federal agency involved with Operation In Our Sites has claimed the seizure actions were part of the domain name seizure initiative, whether on its own or in conjunction with another operation authorized by IPEC in its Joint Strategic Plans.

104. It is important to note that it is very difficult to find a complete compilation of all the seizure actions taken under Operation In Our Sites and that is why this Note focuses on such a task.

105. *See* News Release, U.S. Immigration and Customs Enforcement, "Operation In Our Sites" Targets Internet Movie Pirates, ICE, Manhattan U.S. Attorney Seize Multiple Web Sites for Criminal Copyright Violations (June 30, 2010), *available at* https://www.ice.gov/news/releases/1006/100630losangeles.htm; ANNUAL REPORT 2010,

Center, ICE, and the U.S. Attorney's Office targeted domain names allegedly involved in the illegal online distribution of first-run and other copyright-protected movies and television shows.[106] NinjaVideo.net, a popular website that provided pirated high quality online content for download, was seized during this phase.[107] Over a year later, in September and October 2011, four people tied to the NinjaVideo.net website pled guilty to their involvement in its operation.[108] The IPR Center also seized TVshack.net, a popular linking site, which is a type of website that provides access—or "links"—to other websites where the content is actually hosted.[109] Although the website did not directly offer pirated material by hosting the content, the website's operator, Richard O'Dwyer, a twenty-four-year-old college student from England, was facing possible extradition to the United States for criminal charges of copyright infringement.[110]

---

supra note 57, at 42. Although ICE claimed that only nine websites were seized, IPEC claims that fifty-nine domain names were seized. ANNUAL REPORT 2010, *supra* note 57, at 42. This is because fifty of those sites were parked or unused sites related to one of the other nine seized domain names. ANNUAL REPORT 2010, *supra* note 57, at 42

106. Some of the content that these sites allegedly made available included copies of "The Karate Kid," "Prince of Persia," and "Sex and the City 2." *See* Press Release, U.S. Attorney for the Southern District of New York, Manhattan Federal Court Orders Seizures Of Seven Websites For Criminal Copyright Infringement In Connection With Distribution Of Pirated Movies Over The Internet, at 2 (June 30, 2010), *available at* http://www.justice.gov/usao/nys/pressreleases/June10/websitedomainnameseizurepr.pdf.

107. *See* News Release, ICE, Targets Internet Movie Pirates, *supra* note 105.

108. *See, e.g.*, *Leader of NinjaVideo.net Website Sentenced to 22 Months In Prison For Criminal Copyright Conspiracy*, U.S. ATTORNEY'S OFFICE FOR THE EASTERN DISTRICT OF VIRGINIA PRESS RELEASE (Jan. 6, 2012), *available at* http://www.justice.gov/usao/vae/news/2012/01/20120106ninjavideonr.html (reporting that Hana Amal Beshara was sentenced to serve twenty-two months in prison and repay $209,827 that she personally obtained from her work on NinjaVideo.net); *Co-Founder of NinjaVideo.net Website Sentenced in Virginia to 14 Months in Prison for Criminal Copyright Conspiracy*, U.S. DEPARTMENT OF JUSTICE PRESS RELEASE (Jan. 20, 2012), *available at* http://www.justice.gov/opa/pr/2012/January/12-crm-079.html (reporting that Matthew David Howard Smith was sentenced to serve fourteen months in prison and ordered to repay $172,387).

109. *See* News Release, ICE, Targets Internet Movie Pirates, *supra* note 105; *see also supra* note 101 (describing what a linking site is). "Linking websites are popular because they allow users to quickly browse content and locate illegal streams that would otherwise be more difficult to find." News Release, ICE, New York Investigators, *supra* note 101.

110. *See* Somini Sengupta, *U.S. Pursuing a Middleman in Web Piracy*, N.Y. TIMES, July 12, 2012, http://www.nytimes.com/2012/07/13/technology/us-pursues-richard-odwyer-as-intermediary-in-online-piracy.html?pagewanted=all&_r=0. O'Dwyer is awaiting his appeal of the U.K.'s Home Secretary Teresa May's official approval of the extradition request from U.S. authorities. The appeal is schedule for December 4 at the Royal Courts of Justice in London. *See TV Shack Admin Richard O'Dwyer "Almost Certain" To Be Extradited To US*, TORRENTFREAK (Oct. 25, 2012), http://torrentfreak.com/tv-shack-admin-richard-odwyer-almost-certain-to-be-extradited-to-us-121025/.

The second phase took place in November 2010 to coincide with Cyber Monday[111] and thus was nicknamed the "Cyber Monday Crackdown."[112] ICE investigated online retailers of counterfeit hard goods, like sports equipment, athletic apparel, handbags, and sunglasses, along with DVDs, music, and software—websites that sold goods that people would have otherwise bought as holiday gifts.[113] Dajaz1.com, the popular hip-hop blog whose seizure led to widespread criticism of Operation In Our Sites, was seized during this phase.[114]

On February 1, 2011, ten domain names related to sporting events were seized under the third phase, which purposefully coincided with the NFL's 2011 Super Bowl.[115] The affidavit supporting the seizure warrant describes the websites in question as popular linking sites that allegedly provide access to pirated streaming telecasts of major sporting events that were copyrighted by the NFL, NBA, NHL, WWE, and UFC.[116] The U.S. Attorney for the Southern District of New York, Preet Bharara, explained financial hardships that the sports industry endures when its content is illegally distributed online and noted that this was the policy reason for pursuing the websites.[117] ICE shut down two websites under the Rojadirecta domain name with American registries, despite the domain being declared non-infringing two years prior by a Spanish Court.[118] The struggle of Puerto80, the company that owns the

111. Cyber Monday is a marketing term for the Monday immediately following Black Friday, the Friday following Thanksgiving in the United States. The term was created to persuade people to shop online for holiday gifts.

112. *See* Chaitovitz, *supra* note 20, at 6.

113. *See* News Release, U.S. Immigration and Customs Enforcement, ICE Seizes 82 Website Domains Involved In Selling Counterfeit Goods As Part of Cyber Monday Crackdown (Nov. 29, 2010), *available at* https://www.ice.gov/news/releases/1011/101129 washington.htm; ANNUAL REPORT 2010, supra note 57, at 77.

114. *See* Dajaz1 Affidavit, *supra* note 78. The seizure warrant was solicited in November 2010 during Cyber Monday phase. Dajaz1 Affidavit, *supra* note 78.

115. *See* News Release, ICE, New York Investigators, *supra* note 101.

116. *See* Rojadirecta Affidavit, *supra* note 78, ¶¶ 13–14, 24, 41; News Release, ICE, New York Investigators, *supra* note 101 ("Users simply click on a link to begin the process of downloading or streaming to their own computer an illegal broadcast of a sporting event from the third party website that is hosting the stream.").

117. *See* News Release, ICE, New York Investigators, *supra* note 101 (" 'The illegal streaming of professional sporting events over the Internet deals a financial blow to the leagues and broadcasters who are forced to pass their losses off to the fans in the form of higher priced tickets and pay-per-view events . . . .' ").

118. *See* Brief of Amici Curiae, *supra* note 18, at 13–15 (explaining that the site was declared non-infringing by a Spanish Court two years prior to its seizure in the United States and that the U.S. government should afford more deference to a foreign government's determination under a similar copyright infringement claim).

popular sporting domain Rojadirecta, is a famous example of how difficult it is for owners of seized domain names to recapture their property.[119]

The fourth phase took place a few days later on Valentine's Day 2011.[120] Eighteen domain names allegedly selling luxury counterfeit goods were seized under the name "Operation Broken Hearted."[121] The goods allegedly violated the trademarks of brands such as Breitling, Burberry, Chanel, Coach, Dolce & Gabbana, Gucci, Louis Vuitton, Nike, Omega, Patek Philipe, Prada, Rolex, Tiffany & Co., and Timberland.[122] According to ICE, these were "deals too good to be true."[123]

The fifth phase of Operation In Our Sites took place in May 2011. Five domain names were seized, including three for involvement in the sale of counterfeit goods and two for pirated content.[124] Both ICE and IPEC's official press releases are very vague about this phase.

In July 2011, ICE seized seventeen domain names during its sixth phase, dubbed "Operation Shoe Clerk."[125] These websites were dedicated to the sales of goods allegedly infringing on the trademarks of brands such as Dolce & Gabbana, Gucci, Lacoste, PUMA, and others.[126] Ryan Breen, the operator of one of the seized sites, was arrested and convicted in the Western District of New York for selling counterfeit merchandise relating to the popular television show *Sons of Anarchy*.[127]

The seventh phase, "Operation Strike Out," coincided with the Baseball World Series in October 2011 and involved a month-long investigation of

119. *See supra* Section II.C.2 (discussing the struggles Puerto80 went through to regain their domain names after they were seized); Opening Brief and Special Appendix for Petition-Appellant Puerto 80 Projects, S.L.U., Puerto 80 Projects, S.L.U. v. United States, 11-3390, at 7–9 (2d Cir. Sept. 16, 2011) [hereinafter Opening Brief for Puerto 80] (discussing Puerto 80's attempts to engage the government in negotiations for five months after the government had already seized its two American websites without any notice).

120. *See* News Release, U.S. Immigration and Customs Enforcement, Sweetheart, But Fake, Deals Put On ICE "Operation Broken Hearted" Protects Consumers From Counterfeit Valentine's Day Goods (Feb. 14, 2011), *available at* https://www.ice.gov/news/releases/1102/110214washingtondc.htm.

121. *See id.*

122. *See id.*

123. *Id.*

124. *See* ANNUAL REPORT 2011, supra note 57, at 24, 101.

125. *See* News Release, U.S. Immigration and Customs Enforcement, Homeland Security Investigations Brings Counterfeit Designers to Heel (July 28, 2011), *available at* http://m.ice.gov/news/releases/1107/110728washingtondc.htm?f=m.

126. *See id.* Other Brands include New Era, Nike, The North Face, Oakley, Ralph Lauren, Ray-Ban, Tory Burch, UGG, and the popular T.V. show "Sons of Anarchy." *Id.*

127. *See id.* ("The website offered counterfeit t-shirts for sale using the show's trademark brand without the permission of the Fox Broadcasting Company.").

websites engaging in the sale of allegedly counterfeit sports memorabilia, including websites suspected of violating copyrights and trademarks owned by MLB, NBA, NFL, and NHL.[128] The result of this phase was the seizure of fifty-eight domain names and 5,347 counterfeit items with a Manufacturer's Suggested Retail Price of $134,862.[129]

On November 28, 2011, the second "Cyber Monday"[130] initiative was concluded as the eighth phase of Operation In Our Sites.[131] The government seized 152 websites involved in the sale of allegedly counterfeit merchandise,[132] representing an eighty percent increase in the number of sites seized compared to the first "Cyber Monday."[133]

ICE seized twelve domain names in the ninth phase on December 4, 2011.[134] The websites were aimed at the American-Korean community and were selling allegedly pirated copies of movies, television shows, software, and workout DVDs.[135] Two website operators involved with the domains were arrested and indicted on November 30, 2011.[136]

Operation Fake Sweep, the tenth phase, ran from October 2011 until February 2012.[137] The sweep was a nationwide enforcement effort that took place over several months leading up to the NFL's Super Bowl XLVI.[138] The part of the investigation associated with Operation In Our Sites resulted in the seizure of 307 domain names, including 291 websites selling allegedly

128. *See* News Release, U.S. Immigration and Customs Enforcement, ICE Announces Results of 'Operation Strike Out' (Oct. 31, 2011), *available at* https://www.ice.gov/news/releases/1110/111031washingtondc.htm.

129. *See id.* By the end of October, the banners that replaced the seized domain names had been viewed over seventy-five million times. *Id.*

130. *See supra* note 111 (explaining "Cyber Monday").

131. *See* News Release, U.S. Immigration and Customs Enforcement, Operation In Our Sites Protects American Online Shoppers, Cracks Down on Counterfeiters (Nov. 28, 2011), *available at* https://www.ice.gov/news/releases/1111/111128washingtondc.htm.

132. ICE's initial news release on the eighth phase states that 150 websites were seized but two more sites were seized after the publication of the news release, totaling 152 domain names seized pursuant to the second Cyber Monday. *Id.*

133. *See id.*

134. ICE did not issue an official news release for the seizure as it generally does with every phase of the operation; however, IPEC's Intellectual Property Spotlight December 2011 Edition mentions the seizure and subsequent ICE News Releases acknowledge this phase as the ninth. *See* ANNUAL REPORT 2011, *supra* note 57, at 25, 114.

135. *See* ANNUAL REPORT 2011, *supra* note 57, at 25, 114.

136. *See id.*

137. *See* News Release, U.S. Immigration and Customs Enforcement, Special Agents and Officers Seize More Than $4.8 Million in Fake NFL Merchandise and Seize 307 Websites During 'Operation Fake Sweep (Feb. 2, 2012), *available at* https://www.ice.gov/news/releases/1202/120202indianapolis.htm.

138. *See id.*

counterfeit game-related sportswear and sixteen websites offering allegedly illegal streaming of sporting telecasts.[139]

The DOJ announced the seizure of more than $1.5 million in proceeds from the online sale of counterfeit sports apparel made in China on May 11, 2012.[140] The seizure stemmed from an IPR Center investigation of commercial websites involved in the sale of allegedly counterfeit goods.[141] It is important to note that this operation marked the beginning of ICE and the IPEC stopping the designation of specific seizure actions as separate phases, despite continuing to credit subsequent actions as part of the Operation In Our Sites initiative.

"Project Copy Cat" marked the two-year anniversary of Operation In Our Sites in July 2012, and resulted in the seizure of seventy domain names.[142] The targeted domain names were websites that were designed to copy original websites, so even the most discerning shopper would have a very difficult time differentiating between a counterfeit site and the original site it copied.[143]

August 2012 was the first time that Operation In Our Sites seized domain names related to cell phone applications ("apps").[144] The three domain names seized were allegedly engaged in the illegal distribution of copies of copyrighted Android cell phone apps through alternative online markets.[145] The IPR Center, ICE, DOJ, and FBI coordinated their efforts with international law enforcement, such as the Dutch and French governments, because the servers storing these apps were hosted in other countries.[146] ICE, in justifying its new direction, explained that "software

139. *See id.*

140. *See* Press Release, U.S. Department of Justice, Department of Justice Seizes More Than $1.5 Million in Proceeds from the Online Sale of Counterfeit Sports Apparel Manufactured in China (May 11, 2012), *available at* http://www.justice.gov/opa/pr/2012/May/12-crm-610.html.

141. *See id.*

142. *See* News Release, U.S. Immigration and Customs Enforcement, ICE-Led IPR Center Seizes 70 Websites Duping Consumers Into Buying Counterfeit Merchandise (July 12, 2012), *available at* https://www.ice.gov/news/releases/1207/120712washington.htm.

143. *See id.* ("The 70 websites . . . closely mimicked legitimate websites selling authentic merchandise and duped consumers into unknowingly buying counterfeit goods. Many of the websites so closely resembled the legitimate websites that it would be difficult for even the most discerning consumer to tell the difference.").

144. The sites seized were: applant.net, appbucket.net, and snappzmarket.com. *See* Press Release, U.S. Department of Justice, Federal Courts Order Seizure of Three Website Domains Involved in Distributing Pirated Android Cell Phone Apps (Aug. 21, 2012), *available at* http://www.justice.gov/opa/pr/2012/August/12-crm-1033.html.

145. The sites seized were: applant.net, appbucket.net, and snappzmarket.com. *See id.*

146. *See DOJ/FBI Seize Domain Names*, *supra* note 36.

apps have become an increasingly essential part of our nation's economy and creative culture."[147]

In early October 2012, ICE announced "Project Bitter Pill," an investigation that resulted in the seizure of 686 websites involved in the selling of allegedly illegal counterfeit pharmaceuticals.[148] The two-month-long investigation involved many international actors, such as INTERPOL,[149] and was the largest single seizure action to date under Operation In Our Sites.[150]

ICE continued its trend of cracking down on Cyber Monday by seizing 101 domain names involved in the sale of allegedly counterfeit merchandise online in late November 2012[151] and another eighty-nine websites in December 2012.[152] However, "recognizing the global nature of Internet crime, this year the IPR Center partnered with Europol, who, through its member countries, executed coordinated seizures of foreign-based top-level domains such as .eu, .be, .dk, .fr, .ro and .uk."[153] The result was another thirty-one domain names seizures abroad.[154] ICE Director Morton emphasized that these allegedly infringing sites are part of an international problem that should be addressed through international partnerships.[155]

Although this list of the various seizure actions taken by ICE, IPR Center, and DOJ is long, it is important to emphasize the vast amount of domain names affected across many different types of intellectual property industries. By conceptualizing in one place the various publicized seizure actions, it not only draws upon the breadth of work that Operation In Our

147. Press Release, DOJ, Federal Courts Order Seizure, *supra* note 144.

148. *See* News Release, U.S. Immigration and Customs Enforcement, HIS Seizes 686 Websites Selling Counterfeit Medicine to Unsuspecting Consumers (Oct. 4, 2012), *available at* https://www.ice.gov/news/releases/1210/121004washingtondc.htm.

149. *See id.*

150. The IPR Center and ICE have always claimed authority to seize domain names involved in the sale of counterfeit pharmaceuticals due to the threat to national health and safety. *See* IPR Press Release, *supra* note 64; *see also supra* note 102 and accompanying text. However, this effort was the first time Operation In Our Sites has seized pharmaceutical sites on such a large scale.

151. *See* News Release, ICE, European Law Enforcement Agencies, *supra* note 71 ("These websites were set up to dupe consumers into unknowingly buying counterfeit goods as part of the holiday shopping season.").

152. *See* News Release, ICE, Houston HIS Seizes, *supra* note 3 ("89 domain names were seized. . . . This brings the total number of domain names seized for Cyber Monday to 190. This is the third year that the IPR Center has targeted websites selling counterfeit products online in conjunction with Cyber Monday.").

153. News Release, ICE, European Law Enforcement Agencies, *supra* note 71.

154. *See id.*

155. *See id.* ("Our partnerships enable us to go after criminals who are duping unsuspecting shoppers all over the world. This is not an American problem, it is a global one and it is a fight we must win.").

Sites is responsible for in a mere two and a half years, but also emphasizes how many people may have had their rights implicated.

II. WHAT'S ALL THE FUSS ABOUT? ISSUES SURROUNDING OPERATION IN OUR SITES

Our system of intellectual property rights only functions if there is proper enforcement; however, how to strike a proper balance between enforcement efforts to protect the rights holders and the individual rights of the website operators and their visitors is a hotly contested issue. Although the IPEC created the Joint Strategic Plans to strengthen intellectual property enforcement across federal agencies, Operation In Our Sites's process of seizing domain names without prior notice to website owners has arguably violated constitutional rights. Analyzing the potential (and realized) risks of this process is important in determining whether this enforcement effort is one that is working and that should be continued.

A. CONSTITUTIONAL ISSUES

1. (Lack of) Due Process

The process of seizing domain names under Operation In Our Sites is an *in rem ex parte* forfeiture, which does not afford the website owners any prior notice.[156] However, the opportunity to defend oneself against allegations of wrongdoing prior to the imposition of remedial measures is highly valued in the U.S. Constitution.[157] Due process limits *ex parte* orders to extraordinary circumstances, so only in extreme cases may the government deprive a

156. *See supra* note 21 (defining *in rem*). *Ex parte* is defined as "Done or made at the instance and for the benefit of one party only, and without notice to, or argument by, any person adversely interested; of or relating to court action taken by one party without notice to the other." BLACK'S LAW DICTIONARY (9th ed. 2009).

157. *See* U.S. CONST. amend. V ("No person shall . . . be deprived of life, liberty, or property, without due process of law."); United States v. James Daniel Good Real Prop., 510 U.S. 43, 53 (1993) ("The right to prior notice and a hearing is central to the Constitution's command of due process."); *see also* David Makarewicz, *5 Reasons Why the US Domain Name Seizures Are Unconstitutional*, TORRENTFREAK (Mar. 12, 2011), http://torrentfreak.com/5-reasons-why-the-us-domain-seizures-are-unconstitutional-110312/. Makarewicz explains the importance of due process:

> In many ways, the whole point of due process is to protect citizens from wrongful Government action. The Supreme Court has explained that the right to notice and a hearing prior to a government seizure is for the purpose of enabling an individual "to protect his use and possession of property from arbitrary encroachment-to minimize substantively unfair or mistaken deprivations of property."

Id.

person of his or her property without advance notice and a hearing.[158] When the government seizes a domain name, the constitutionality of the seizure turns on whether the notice and hearing required by the Constitution must occur before or after the seizure takes place.[159]

Supporters of the *in rem ex parte* seizure process emphasize that domain names are a type of property that constitutes an extraordinary situation, such that no prior notice is required.[160] First, the public has an interest in preventing the continued use of websites that are allegedly engaged in criminal copyright violations or distributing counterfeit goods.[161] Second, there is a special need to keep the website owners in the dark about the pending seizure because the nature of domain names makes them transient; website owners can move them out of the jurisdictional reach of ICE under the Pro IP Act or can destroy the domain names before the government commences civil forfeiture proceedings.[162] Third, government officials in the DOJ, ICE, and the IPR Center—not self-interested parties—are initiating the seizures.[163] Supporters within the federal government seem content with

158. *See* Fuentes v. Shevin, 407 U.S. 67, 90–91 (1972). The *Fuentes* Court explained why *ex parte* orders are generally reserved for extraordinary situations:

> There are 'extraordinary situations' that justify postponing notice and opportunity for a hearing. These situations, however, must be truly unusual. Only in a few limited situations has this Court allowed outright seizure without opportunity for a prior hearing. First, in each case, 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.

Id. (citations omitted).

159. *See* Hart, *supra* note 30.

160. *See Fuentes*, 407 U.S. at 90–91 (discussing the three unusual circumstances that qualify for seizure without prior notice and hearing).

161. *See* Hart, *supra* note 30. Hart explains why domain names fall under *Fuentes'* three-factors:

> The seizure permits the US "to assert *in rem* jurisdiction over the property in order to conduct forfeiture proceedings, thereby fostering the public interest in preventing continued illicit use of the property and in enforcing criminal sanctions", domain names "could be removed to another jurisdiction, destroyed, or concealed, if advance warning of confiscation were given", and "seizure is not initiated by self-interested private parties", but by federal officials.

Id.

162. *See id.*

163. *See id.*

the fact that, due to these factors, a neutral magistrate's determination that there is probable cause to seize the domain name is the only due process required.[164] Lastly, supporters of the process claim that seizing domain names poses less risk than seizing other types of real property. Since the domain name seizure leaves the IP address of the website intact, the website owner and his visitors can still access the website's content after seizure has occurred.[165]

On the other hand, in an open letter to ICE, Senator Ronald Wyden expressed his concerns with the way Operation In Our Sites has functioned on the ground. He emphasized that the operation does not afford those whose domain names have been seized a proper means to defend themselves and the content on their websites.[166] Senator Wyden "worr[ied] that domain name seizures could function as a means for end-running the normal legal process in order to target websites that may prevail in full court."[167] This is especially true given that it is unclear if website operators can be liable when the website's users post the infringing content, or when another site—to which the operator merely links—hosts the infringing content.[168]

---

164. *See* Makarewicz, *supra* note 157 (discussing the exchange between IPEC Victoria Espinel and Congresswoman Zoe Lofgren at a House Judiciary Subcommittee on Intellectual Property, Competition, and the Internet). "Espinel attempted to argue that a judge's sign off amounted to due process. Lofgren tersely countered by saying 'With all due respect, judges sign a lot of things.' " *Id.*

165. *See* Hart, *supra* note 30. Some would argue that seizures of domain name do not pose any extra risk:

> The "risk of error" involved in seizing domain names is no higher than those involved in the seizure of personal property: 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.

Id.; *see also supra* note 84 (explaining that when the government seizes a domain name it requires the domain name registry to redirect the domain name to an IP address that displays the government banner; however, the website can still be accessed by typing in the original IP address).

166. *See* Letter from Sen. Ron Wyden to John Morton, *supra* note 6.

167. *Id.*

168. *See* Flava Works, Inc. v. myVidster.com, 689 F.3d 754 (7th Cir. 2012) (explaining the plaintiff video producer was not likely to succeed against a social bookmarking website because in its contributory copyright infringement claim, where the defendant did not induce or significantly increase the amount of infringement); *see also* Mike Masnick, *Rojadirecta Points Court to FlavaWorks Ruling Concerning Infringement On Linking Sites*, TECHDIRT (Aug. 14, 2012, 8:24 PM), http://www.techdirt.com/articles/20120814/00493120013/rojadirecta-points-court-to-flavaworks-ruling-concerning-infringement-linking-sites.shtml ("Even if they don't quite agree with Posner's ruling [in *Flava Works v. myVidster*], just the fact that there are significant questions over whether or not linking/embedding are legal, should raise

Other opponents have also noted that the lack of prior notice and full adversarial hearing increases the likelihood of an improper seizure.[169] David Sohn, Senior Counsel for CDT explains that "[w]hen law enforcement makes its case unopposed and a domain name owner has no opportunity to defend itself, mitigating factors and overbreadth issues may not come to light before the name is seized of blocked. In a one-sided process, the risk of mistakes or overaggressive action is high."[170] Although not officially part of Operation In Our Sites, ICE's actions in seizing 84,000 websites that it falsely believed to be engaged in child pornography under "Operation Save Our Children" is a telling tale of the high risk and overbreadth of the *ex parte* forfeiture process.[171] In February 2011, ICE seized the domain name mooo.com that allows users to register free subdomains in the form of "username.mooo.com," which hosts many personal and small business websites."[172] Because of ICE's failure to realize that the subdomains were entirely distinct from each other, its actions in seizing the parent domain of mooo.com in an attempt to seize one subdomain name suspected of child pornography resulted in the blocking of thousands of innocent websites whose visitors were wrongfully told that the website they were visiting hosted the obscene content.[173] This is merely one example of many instances in which the lack of due process adversely affects website owners and visitors.

2. Free Speech and Prior Restraint

Some of the targeted websites not only served copyrighted content and counterfeit goods, but also contained legitimate, lawful speech, including

significant questions about the "willfulness" needed to show criminal copyright infringement.").

169. *See Promoting Investment and Protecting Commerce Online: Legitimate Sites v. Parasites. Part 1: Hearing Before the H. Comm. on the Judiciary, Subcomm. on Intellectual Property, Competition, and the Internet*, 112th Cong. 37 (2011) [hereinafter *Online Commerce Hearing I*] (statement of David Sohn, Senior Policy Counsel, Center for Democracy & Technology), *available at* http://judiciary.house.gov/hearings/hear_03142011.html.

170. *Id.*

171. *See* Ernesto, *U.S. Government Shuts Down 84,000 Websites, 'By Mistake,'* TORRENTFREAK (Feb. 16, 2011), http://torrentfreak.com/u-s-government-shuts-down-84000-websites-by-mistake-110216/ ("The above failure again shows that the seizure process is a flawed one, as has been shown several times before in earlier copyright infringement sweeps. If the Government would only allow for due process to take place, this and other mistakes wouldn't have been made.").

172. *See* Brief of Amici Curiae, *supra* note 18, at 4–5.

173. *See id.* Website visitors were informed through the use of a similar banner system as Operation In Our Sites, however these banners indicated that child pornography was the reason for the seizure. *See* WIKIPEDIA OPERATION PROTECT OUR CHILDREN BANNER, https://en.wikipedia.org/wiki/File:Operation_Protect_Our_Children_banner.jpg (last visited Jan. 22, 2012).

conversations from chat rooms and posts in discussion forums and blogs. Although the First Amendment does not protect infringing content,[174] legitimate, uninfringing speech should be afforded the full protection granted by the Constitution. The First Amendment has in place substantive and procedural safeguards to help protect speech that is legitimate while enjoining content that is infringing.[175] The issue then becomes whether the civil forfeiture provision of the Pro IP Act and its process of seizing domain names without any prior notice and only based on a mere showing of probable cause violates the First Amendment protection of free speech.[176]

Opponents of Operation In Our Sites's method of seizing domain names prior to any adversarial hearing have claimed that this process can amount to a type of censorship because these are websites that contain some lawful content, rather than just criminal items, warranting more due process protection in order to comply with the First Amendment.[177] This is

174. *See* Eldred v. Ashcroft, 537 U.S. 186, 221 (2003) (holding that copyright's safeguards are adequate to cover First Amendment concerns); Harper & Row, Publishers, Inc. v. Nation Enters., 471 U.S. 539, 555–60 (1985) (same); Mark A. Lemley & Eugene Volokh, *Freedom of Speech and Injunctions in Intellectual Property Cases*, 48 DUKE L.J. 147, 150 (1998) ("[T]he Supreme Court has held that copyright law is a constitutionally permissible speech restriction; though copyright law restricts what we can write or record or perform, the First Amendment doesn't protect copyright-infringing speech against such a restraint.").

175. *See* Henry P. Monaghan, *First Amendment "Due Process*,*"* 83 HARV. L. REV. 518, 518 (1970) ("[C]ourts have begun to construct a body of procedural law which defines the manner in which they and other bodies must evaluate and resolve first amendment claims—a first amendment "due process," if you will."). "It is in the obscenity area that the courts have been most concerned with procedural matters. There the Supreme Court has fashioned a series of specific rules designed to prevent insensitive procedural devices from strangling first amendment interests." *Id.* at 518. Monaghan identifies the First Amendment procedural test as whether the procedure shows "the necessary sensitivity to freedom of expression." *Id.* at 519.

176. *See generally id.* at 532–39 (discussing first amendment "due process" as applied to *ex parte* seizures).

177. *See* Statement of Rep. Zoe Lofgren, Lofgren, Wyden Question Response to Seizure Inquiries, *available at* http://lofgren.house.gov/index.php?option=com_content&view=article&id=637&Itemid=130. Representative Lofgren is one of the most vocal advocates against Operation In Our Sites in Congress. She explains:

> ICE's response fails to address legitimate concerns about "Operation In Our Sites." Domain seizures without due process are a form of censorship. In this instance, our government has seized domains with nothing more than the rubber stamp of a magistrate, without any prior notice or adversarial process, leaving the authors of these sites with the burden of proving their innocence. While this might be enough for the seizure of stolen cars or knock-off handbags, it is not enough for web sites and speech on the Internet. It is disturbing that this administration is treating them the same.

Id.

particularly the case with the seizure of linking sites, websites that do not host the allegedly infringing content but rather contain speech that encourages its visitors to click on links that will lead them to third-party sites that host the infringing content.[178] Since the seizures take down entire websites rather than target specific unlawful content, ICE's domain name seizure methods can amount to a violation of an innocent party's First Amendment right to free speech in cases where different individuals author different parts of the website.[179]

The First Amendment not only protects the right to distribute legal speech, but also "necessarily protects the right to receive it."[180] The websites targeted under Operation In Our Sites all had visitors from the United States, thus implicating those visitors' rights when a site with lawful content was seized.

More importantly, seizure of protected speech without a prior determination that the content is infringing can amount to a prior restraint under the Constitution.[181] Prior restraints are extremely "serious and the least tolerable infringement on First Amendment rights" and are highly disfavored by our jurisprudence.[182] When an item to be seized involves speech, rather than just a tangible instrumentality of the illegal action, more due process is required to make sure that the First Amendment safeguards are not violated. The Court has held "that mere probable cause to believe a legal violation has transpired is not adequate to remove books or films from circulation."[183] Thus, by analogy to the online context, the mere showing of probable cause required under the civil forfeiture provisions of the Pro IP Act is not enough to guard against First Amendment concerns that are unique to domain

178. *See supra* note 101 (describing what a linking site is).

179. *See Online Commerce Hearing I*, *supra* note 169, at 9 (statement of David Sohn, Senior Policy Counsel, Center for Democracy & Technology). Seizures can affect both "lawful and unlawful content, including non-Web content like email or instant messaging connections." *Id.*

180. Martin v. City of Struthers, 319 U.S. 141, 143 (1943). This First Amendment right to receive free speech applies to content delivered over the Internet as well. *See* Reno v. ACLU, 521 U.S. 844, 874 (1997).

181. *See* Hart *supra* note 30. Infringing content is not protected by the First Amendment. *Id.* "The term 'prior restraint' is used to describe administrative and judicial orders *forbidding* certain communications when issued in advance of the time that such communications are to occur." Alexander v. United States, 509 U.S. 544, 550 (1993).

182. Neb. Press Ass'n v. Stuart, 427 U.S. 539, 559 (1976). *See also* Bantam Books, Inc. v. Sullivan 372 U.S. 58, 70 (1963) ("Any system of prior restraints of expression comes to this Court bearing a heavy presumption against its constitutional validity. . . . We have tolerated such a system only where it operated under judicial superintendence and assured an almost immediate judicial determination of the validity of the restraint." (citations omitted)).

183. Fort Wayne Books, Inc. v. Indiana, 489 U.S. 46, 66 (1989).

names. In order to comply with the First Amendment, a judicial determination as to whether the domain names contained infringing material needed to be made, not just a magistrate's determination that there exists probable cause that such material exists on the site.[184] The Court has explained that in order for a prior restraint by an administrative agency to be constitutional, the process of seizing the speech "must include: (a) an adversarial hearing, (b) with the burden on the censor, and (c) with clear opportunity for prompt judicial review and appeal."[185]

Proponents of Operation In Our Sites compare the seizure of websites engaged in allegedly illegal conduct to the confiscation of obscene materials and argue that these seizures are thus consistent with the strictures of the First Amendment.[186] Since the First Amendment does not protect obscene materials,[187] these materials would be akin to infringing speech and courts should follow the same analysis in determining if the seizure violates First Amendment protections.

In making sure that the seizure of obscene content does not amount to a seizure of lawful speech as well, courts must ensure that the government has met two requirements.[188] First, the seizure of the obscene material must comply with the Fourth Amendment, which requires that the government "describe the targeted material with specificity" in the instrument granting seizure.[189] Supporters argue that Operation In Our Sites obviously meets this requirement because the government seizes the domain names pursuant to "valid, specific warrants" based on probable cause issued by a neutral magistrate, who makes an independent determination from information contained in a sworn affidavit.[190]

The Supreme Court has also indicated that it treats seizures done for preservation of evidence differently from forfeiture, regarding the former as

184. *See* Brief of Amici Curiae, *supra* note 18, at 12.

185. *Id.* at 11.

186. *See* Chaitovitz *supra* note 20, at 11–12.

187. *But see* Miller v. California, 413 U.S. 15, 23–24 (1973) (expressing concern about categorically stating that no obscene content is protected and trying to limit state-obscenity laws).

188. *See* Chaitovitz *supra* note 20, at 11–12.

189. *See id.* at 11; s*ee also* Stanford v. Texas, 379 U.S. 476, 485 (1965) ("[T]he constitutional requirement that warrants must particularly describe the 'things to be seized' is to be accorded the most scrupulous exactitude when the 'things' are books, and the basis for their seizure is the ideas which they contain.").

190. Hart, *supra* note 30 ("There is no question that the government has met this requirement; the seizures were made pursuant to valid, specific warrants issued by a neutral, impartial judge.").

more permissible.[191] Given that a website's content is still accessible after the domain name seizure by typing in the site's IP address, this type of *in rem* seizure falls into the more permissible category. Further, ICE has claimed that the seizure takes place in order to preserve the domain name for the civil forfeiture proceeding, guarding against the possibility that the website owner may take the site down or transfer it beyond the jurisdictional reach of § 2323 if he were afforded prior notice.[192]

The second procedural requirement mandates a judicial determination of whether to impose a final restraint of speech,[193] but supporters claim this determination does not need to occur before the seizure.[194] Since the seizure occurs to preserve the property for the forfeiture proceeding, which must take place within a statutorily mandated period of time,[195] and the website owner can challenge the seizure, proponents argue that Operation In Our Sites meets this second procedural requirement.[196] Proponents also point out that the domain name seizure does not amount to censorship and thus cannot be a final restraint because the website's content can still be accessed by using the site's IP address and the website owner can set up a new domain.[197] However, this argument is somewhat odd because, on one hand, it assumes that a seizure is required in order to preserve the domain name for

191. *See* Heller v. New York, 413 U.S. 483, 492 (1973)

> [S]eizing films to destroy them or to block their distribution or exhibition is a very different matter from seizing a single copy of a film for the bona fide purpose of preserving it as evidence in a criminal proceeding, particularly where, as here, there is no showing or pretrial claim that the seizure of the copy prevented continuing exhibition of the film.

Id.

192. *But see* Makarewicz, *supra* note 157 (arguing that domain names should be regarded more like real estate that cannot be moved because "A domain . . . cannot be moved or concealed from the Government without defeating the purpose of having a domain in the first place.").

193. *See* Chaitovitz, *supra* note 20, at 12.

194. *See Heller*, 413 U.S. at 489. In prior civil forfeiture cases, in which the government aimed to ultimately suppress the targeted material, the Court "did not require that the adversary proceeding must take place prior to *initial* seizure. Rather, it was held that a judicial determination must occur 'promptly so that administrative delay does not in itself become a form of censorship." *Id.*

195. *See* 18 U.S.C. § 983(a)(1) (2006) (mandating that the government must send written notice of the seizure or file a civil judicial forfeiture action within 60 days of the date of seizure).

196. Hart, *supra* note 30 ("This does not mean that a judicial determination must occur *before* seizure. The Court in *Heller v. New York* said . . . 'a judicial determination need only occur "promptly so that administrative delay does not in itself become a form of censorship." ' ").

197. *See id.* (comparing the seizure of domains to the lawful seizure of the film in *Heller*, stating that domain name seizures are "even less like a form of final restraint").

the forfeiture proceeding while, on the other hand, it assumes that the website owner still has full control over his or her website's content through its IP address. It seems that proponents of Operation In Our Sites are trying to claim two different stances whenever it is convenient for their argument.

B. OTHER CONCERN: LINKING SITES CANNOT BE LIABLE FOR CRIMINAL COPYRIGHT INFRINGEMENT UNDER 17 U.S.C. § 506

Websites that only induce or facilitate copyright infringement—such as linking sites, which only post links to other websites that host the illegal content—are not direct infringers and thus fall outside the scope of criminal copyright law.[198] Although websites for such activities can be held civilly liable for contributory infringement, there is no recognized principle of secondary liability in criminal copyright law. Websites like Dajaz1 and Rojadirecta, along with many other sites accused of criminal copyright infringement, are merely linking sites, and thus very shaky authority exists for these seizures under § 2323 power.

Under § 2323(a)(1)(B), property that was used in facilitating or committing criminal copyright infringement is subject to forfeiture.[199] The purpose of this statute is to hold the property until the owner's conviction and then forfeit the property if the owner is convicted. Therefore, one's property should not be seized pursuant to a forfeiture statute when he or she cannot be convicted of committing the relevant crime under that statute. Although the practical realities of domain name seizures is that a lot of these websites are operated from abroad[200] and thus out of the jurisdictional reach of § 2323 (which is why the statute allows for service on the American domain name registry), it should still follow that the domain names that are subject to forfeiture should only be those that if the operators were within the United States, they would be subject to *criminal* intellectual property violations.

198. *See* 17 U.S.C. § 506(a)(1)(C) (2006). The argument that these linking sites fall under § 506(a)(1)(C), criminal copyright infringement, is very shaky. The "making available" theory of criminal copyright infringement would be wrong because the third-party websites that actually host the infringing content are the sites that "made available" the content in question. *Id.* Rather, it is a better argument that these sites were used to "facilitate the commission of" a § 506 violation by using language and hyperlinks to indicate where the site's visitor could find the infringing content online. *See* 18 U.S.C. § 2323(a)(1)(B) (2006).

199. *See* 18 U.S.C. § 2323(a)(1)(B).

200. *See* Chaitovitz, *supra* note 20, at 12–13 (noting many of the domain names are operated abroad).

C. SPECIFIC EXAMPLES

The domain name seizures of Dajaz1 and Rojadirecta are worth noting. Both sites were seized in the early stages of Operation In Our Sites, and both owners diligently and consistently fought ICE agents, DOJ attorneys, and the IPR Center while attempting to get anyone from the government to speak to them about the status of their seizure and to regain their domains. After prolonged struggles of over a year for each domain, both sites ultimately prevailed in recapturing their websites, despite reduced website traffic that has nearly crippled them. However, their struggles were not in vain because they have shed much-needed light on the unconstitutionality of the process that currently plagues domain names seized pursuant to Operation In Our Sites. Public support for seized domains has centered around the struggles these domains faced, and their advocates have pressed Espinel, Director of ICE Morton, Attorney General Holder, and other key individuals to make domain name seizures follow constitutional and legal norms by incorporating greater transparency in the take-down process.

1. Dajaz1

Dajaz1 is a popular hip-hop blog, which was seized in November 2011 for providing links to four copyrighted songs.[201] However, Dajaz1 was not only a linking site, as described in the affidavit supporting the seizure warrant, but it also served as a blog and place for visitors to post commentary on their favorite artists and rappers.[202] The seizure of the site not only prevented access to the allegedly infringing songs—which were later found to be posted legally with the consent of the rights holders[203]—but also

201. *See* Masnick, *Breaking News*, *supra* note 34; Masnick, *More & Bigger Mistakes*, *supra* note 22. The four songs include: (1) *Deuces*, by Chris Brown; (2) *Long Gone*, by Nelly; (3) *Fall For Your Type*, by Jamie Fox; (4) *Mechanics*, by Reek Da Villian. Masnick, *More & Bigger Mistakes*, *supra.*

202. *See* Masnick, *Breaking News*, *supra* note 34. On his blog, Masnick follows the Dajaz1 case diligently and notes:

> Those seizures struck us as particularly interesting, because among the sites seized were a bunch of hip hop blogs, including a few that were highly ranked on Vibe's list of the top hip hop blogs. These weren't the kinds of things anyone would expect, when supporters of these domain seizures and laws like SOPA and PROTECT IP talk of 'rogue sites.' Blogs would have lots of protected speech, and in the hip hop community these blogs, in particular, were like the new radio.

Id.

203. *See* Masnick, *Breaking News*, *supra* note 34. The nature of the music industry in the Internet age is now:

> Artists routinely leaked their works directly to these sites in order to promote their albums .... The Dajaz1 case become particularly

to the many legitimate and protected blogs hosted on the domain. Access to the commentary on hip-hop was disabled as part of the seizure due to ICE's policy of taking down the entire domain rather than targeting the suspected content.

ICE Agent Andrew Reynolds, a recent college graduate, based his claims of criminal copyright infringement on information he learned from Carlos Linares, VP of Anti-Piracy Legal Affairs for the RIAA.[204] In the affidavit, Reynolds claimed that the songs were in "pre-release" and not authorized for third party distribution over the Internet.[205] To support his claim, Reynolds relied on information he learned from RIAA representatives.[206] What Reynolds failed to realize was that each of the four songs were sent to Dajaz1.com by each perspective rights holder for the purpose of promoting the song.[207] One of the songs listed as infringing was not even represented by the RIAA record label, meaning that Reynolds was not justified in relying on Linares's statement regarding that specific song.[208] Despite this, a magistrate judge granted a seizure order that was served on the domain name registry, requiring it to redirect the domain name to a government IP address displaying the banner that the site engaged in criminal copyright infringement and was seized pursuant to 18 U.S.C. § 2323.

In general, the take-down process for Operation In Our Sites requires that the government notify the website's owner of the seizure within sixty days, which then triggers the owner's right to file a claim in order to contest the seizure.[209] The government then has ninety days to commence a forfeiture proceeding.[210] Although this process is prescribed in the Pro-IP Act, this is not what Dajaz1's lawyer, Andrew Bridges, encountered.[211]

> interesting to us, after we saw evidence showing that the songs that ICE used in its affidavit as 'evidence' of criminal copyright infringement were songs sent by representatives of the copyright holder with the request that the site publicize the works—in one case, even coming from a VP at a major music label.

Id.; *see also* Masnick, *More & Bigger Mistakes*, *supra* note 201.

204. *See* Masnick, *More & Bigger Mistakes*, *supra* note 201.

205. *See* Dajaz1 Affidavit, *supra* note 78, at 56.

206. *See id.*

207. *See* Masnick, *More & Bigger Mistakes*, *supra* note 201.

208. *See* Masnick, *Breaking News*, *supra* note 34 ("In fact, one of the songs involved an artist not even represented by an RIAA label, and Linares clearly had absolutely no right to speak on behalf of that artist.").

209. *See supra* notes 89–91 and accompanying text.

210. *See* 18 U.S.C. § 983(a) (2006) (establishing the steps and durational requirements of seizing and forfeiting under 18 U.S.C. § 2323); Section I.C.2 (describing the process of seizing a domain name).

211. *See* Masnick, *Breaking News*, *supra* note 34.

Rather, the government stalled when contacted by Dajaz1's representatives.[212] However, Dajaz1 was able to file its administrative claim on February 15, 2011, requiring that the government file its forfeiture claim no later than May 16, 2011.[213] After filing this claim, Bridges was informed that the government would begin forfeiture proceedings, but the deadline came and went without notice to anyone at Dajaz1.[214] The government had been seeking secret extensions from the court in order to continue its investigation.[215] It claimed that the order must be kept under seal and that Dajaz1 needed to be kept in the dark because the "filing of a complaint would require the government to reveal . . . information concerning the on-going criminal investigation. The disclosure of that information would likely have an adverse effect on the investigation, if for no other reason than it would indicate that direction and scope of the investigation."[216] Despite incessantly trying to find out any information about the status of Dajaz1, Bridges was left in the dark. He was told that he would just need to trust the government's word; he could not get a redacted version of the order or any information proving that the government actually got three extensions until mid-November 2011.[217]

In the end, despite extending the forfeiture deadline nearly six months, the government decided not to commence the forfeiture process.[218] After Bridges continually asked what the status of the domain name was, the government eventually handed back Dajaz1.com to its owner on December 8, 2011, a month after the last extension expired and over a year after the

212. *See id.* ("After continuing to stall and refusing to respond to Dajaz1's filing requesting the domain be returned, the government told Dajaz1's lawyer, Andrew P. Bridges, that it would begin forfeiture procedures. . . . Then, the deadline for the government to file for forfeiture came and went and nothing apparently happened.").

213. *See* Ex Parte Application For Order Extending For Sixty Days the Deadline For Filing Complaint For Forfeiture at 5, In the Matter of the Seizure of The Internet Domain Name "Dajaz1.com," No. 11-00110 (C.D. Cal. Sept. 8, 2011) [hereinafter Ex Parte Application].

214. *See* Masnick, *Breaking News*, *supra* note 34.

215. *See id.*

216. Ex Parte Application, *supra* note 213, at 5; *see* Masnick, *Breaking News*, *supra* note 34 ("The initial (supposed) secret extension was until July. Then it got another one that went until September. And then *another one* until November . . . or so the government said. When Bridges asked the government for *some proof* that is had actually obtained the extension in question, the government attorney told Bridges that he would just have to 'trust' him.").

217. *See* Ex Parte Application, *supra* note 213.

218. *See* Masnick, *Breaking News*, *supra* note 34.

original seizure of the site.[219] With that came no explanation or apology; rather, the EFF, Wired, and the California First Amendment Coalition worked to get the court documents unsealed, which finally happened in May 2012.[220] The documents reveal that the delay in initiating forfeiture proceedings against Dajaz1 was due to ICE agent Reynolds waiting to hear back from representatives at the RIAA for evidence that the posting of the songs on Dajaz1.com constituted infringement.[221] Opponents of Operation In Our Site's process criticize ICE for seizing Dajaz1 "based on the say-so of the record company guys, and getting secret extensions as they wait for their masters, the record companies, for evidence to prosecute."[222]

As it turned out, the probable cause that Agent Reynolds obtained was a few unsupported statements from a record label executive, which was enough to shut down a popular website for over a year, effectively denying the owners their due process and the site's visitors their First Amendment rights. Dajaz1's attorney, Bridges, criticized the government's actions as "unjustified."[223] Among many points, Bridges compares the seizure of Dajaz1 "to seizing a printing press of the New York Times because the newspaper, in its concert calendar, refers readers to four concerts where the promoters of those concerts have failed to pay ASCAP for the performance licenses."[224] Although the government has never conceded that their actions violated any

219. *See id.* ("[T]he government decided that it would not file a forfeiture complaint . . . and it let the last (supposed) extension expire. Only after Bridges asked *again* for the status of the domain did the government indicate that it would return the domain to its owner.").

220. *See* Mike Masnick, *Judge Lets Feds Censor Blog For Over A Year So The RIAA Could Take Its Sweet Time*, TECHDIRT (May 3, 2012, 4:08 PM), http://www.techdirt.com/articles/20120502/16575418746/judge-lets-feds-censor-blog-over-year-so-riaa-could-take-its-sweet-time.shtml.

221. *See* David Kravets, *Feds Seized Hip-Hop Site for a Year, Waiting for Proof of Infringement*, WIRED (May 3, 2012, 5:00 PM), http://www.wired.com/threatlevel/2012/05/weak-evidence-seizure/.

222. *Id.* (quoting EFF's legal director, Cindy Cohn). Cohn goes on to comment that "[t]his is the RIAA controlling a government investigation and holding it up for a year." *Id.* The RIAA, on the other hand, tried to downplay its involvement in the investigation by stating, "ICE conducted its own independent investigation of the site and ICE along with the Justice Department concluded that there was a basis for seizing the domain name. Rights holders and the RIAA were requested to assist law enforcement and made every attempt to do so in a complete and prompt manner." Masnick, *RIAA Tries To Downplay Its Role*, *supra* note 2.

223. *See* Masnick, *RIAA Tries To Downplay Its Role*, *supra* note 2 (quoting Andrew Bridges).

224. *Id.*

legal or constitutional norms,[225] the Dajaz1 case makes it clear that the federal agents running Operation In Our Sites have not been transparent about whether the website operators are seeking and obtaining the proper process that § 2323 is supposed to afford.

2. Rojadirecta

There are other examples of websites that successfully, yet laboriously, regained their domain name after ICE and the IPR Center seized it. Rojadirecta, for example, is a Spanish sports website owned by Puerto 80, registered with the American company GoDaddy.com, Inc.[226] Pursuant to the third phase of Operation In Our Sites, Rojadirecta was seized on February 1, 2011, under the authority of a warrant issued the by a magistrate judge in the Southern District of New York.[227] According to the affidavit filed in support of seizure, Rojadirecta was targeted because it was a linking site that offered access to third-party websites that contained infringing broadcasts.[228] The warrants were based on ICE's determination that there was enough evidence to amount to probable cause that Rojadiecta had "been used to commit and facilitate criminal copyright infringement."[229] The difference between Dajaz1's case and Rojadirecta's is that after repeated negotiations between Rojadirecta's representatives and the government failed,[230] Rojadirecta decided to sue the government to return their domains, in which the government retaliated by immediately filing to forfeit the

225. *See* Kravets, *supra* note 221 ("The Los Angeles federal prosecutor [in the Dajaz1 case] . . . agreed to unseal the documents, but . . . did so without conceding there was any First Amendment or common law necessity to do so.").

226. *See* 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 2, Puerto 80 Projects, S.L.U. v. United States, No. 11-3983 (S.D.N.Y. 2011), *appeal granted*, No. 11-3390 (2d Cir. Aug. 19, 2011). Both Rojadirecta.com and Rojadirecta.org were seized but are discussed in the singular "Rojadirecta" because both sites are associated with the same IP address and are virtually the same. *See* Rojadirecta Affidavit, *supra* note 78, ¶ 40(a).

227. *See supra* Section I.C.3 (discussing phase three of Operation In Our Sites); News Release, ICE, New York Investigators, *supra* note 101.

228. *See* Rojadirecta Affidavit, *supra* note 78, ¶¶ 40–44. The affidavit goes on to say that Rojadirecta "provides links to daily live sporting events and Pay-Per-View events, as well as downloadable sporting events or Pay-Per-View event that were previously aired." *Id.* ¶ 40(a).

229. *Id.* ¶ 46.

230. See Opening Brief for Puerto 80, *supra* note 119, at 7–9 (offering a detailed account of every attempt of Rojadirecta's attorneys to engage the government agencies involved in discussions and asking the court for a speedy process to regain control of its domains because the government's actions in stalling had caused significant harms to its business).

domains.[231] After two simultaneous legal cases and much arguing back and forth between Rojadirecta's representatives and DOJ attorneys, the government filed a voluntary dismissal notice on August 29, 2012, nearly eighteen months after the original seizures.[232]

Rojadirecta's counsel, intellectual property scholars Mark Lemley and Ragesh Tangri, set out many arguments in both legal proceedings. First, they argued that due to the nature of Rojadirecta's site, which is not just a linking site but also contains lawful speech, seizing the site without a prior determination of its validity constitutes a prior restraint under the First Amendment's Free Speech Clause.[233] Furthermore, they point out that since Rojadirecta is a linking site, it does not host any of the allegedly infringing content on its domain. Under established case law, mere linking to a site does not qualify as criminal copyright infringement because there is a higher pleading requirement of willfulness that cannot be met by indirect copyright infringement.[234] Also, they point out that Rojadirecta was declared non-infringing by two Spanish courts and that this court should not disregard that in order to uphold generally accepted international norms.[235]

III. CONCLUSION AND THE FUTURE

Protecting intellectual property is essential for promoting the United States's economy, health, and safety, as well continuing the country's position as a powerful leader in the world community. Espinel had it right when she explained that intellectual property is one of the largest and most powerful sectors of our economy. And there is no doubt that the Internet is

231. Mike Masnick, *Feds Tie Themselves In Legal Knots Arguing For Domain Forfeiture In Rojadirecta Case*, TECHDIRT (May 16, 2012, 10:22 AM), https://www.techdirt.com/articles/20120516/05031118941/feds-tie-themselves-legal-knots-arguing-domain-forfeiture-rojadirecta-case.shtml.

232. Mike Masnick, *Oops: After Seizing & Censoring Rojadirecta For 18 Months, Feds Give Up & Drop Case*, TECHDIRT (Aug. 29, 2012, 12:45 PM), https://www.techdirt.com/articles/20120829/12370820209/oops-after-seizing-censoring-rojadirecta-18-months-feds-give-up-drop-case.shtml.

233. Opening Brief for Puerto 80, *supra* note 119, at 15–17; *see* Mike Masnick, *Rojadirecta Sues US Government, Homeland Security & ICE Over Domain Seizure*, TECHDIRT (June 13, 2011, 12:22 PM), https://www.techdirt.com/articles/20110613/12021514673/rojadirecta-sues-us-government-homeland-security-ice-over-domain-seizure.shtml (quoting Rojadirecta's brief in its suit filed against the government).

234. Masnick, *Oops*, *supra* note 232 ("Furthermore, the filing points out that the government totally failed to meet the requirements to show criminal copyright infringement, and notes that the government cannot show that Rojadirecta meets those requirements.").

235. Opening Brief for Puerto 80, *supra* note 119, at 14; *see also* Brief of Amici Curiae, *supra* note 18, at 13–14.

responsible for the great growth in online piracy and counterfeiting that plagues our current day and age. Finding a way to deal with this issue is crucial, yet complex.

Operation In Our Sites was the Obama Administration's partial solution to this growing problem. Although the process may not be perfect as the above discussion of possible constitutional concerns and other issues illustrates, it is a valid concern that most of these website operators are abroad or untraceable or can take their site and move it to another jurisdiction and need to be taken into account. By providing for an *in rem ex parte* forfeiture proceeding that begins with no-prior notice seizure, the IPR Center, ICE, and DOJ are trying to do their best to combat online infringement. Although this system may not be perfect, if the DOJ, ICE, and IPR Center follow the Act's mandates of a specific process of steps with durational limitations, constitutional concerns will be mitigated. Technically, *in rem ex parte* forfeiture has been in U.S. common law for centuries and using it in the online context is a new application of it.

An additional solution would be to offer those affected more transparency. By requiring these agencies to answer questions about that status of the seized domains while adhering to statutory timelines and requirements, constitutional violations would be less likely to arise. In order to ensure these agencies are complying with the need for greater transparency, a penalty that the domain would be automatically returned and no forfeiture proceeding could be filed could be imposed if any violations occur. However, because the current process is replete with constitutional violations—both for website owners and visitors—the Obama Administration should require that the agencies executing the operation establish measures that increase transparency and allow website owners to contest allegations in a manner that complies with due process.