

Boston University School of Law

Scholarly Commons at Boston University School of Law


Faculty Scholarship

2011

The In Rem Forfeiture of Copyright-Infringing Domain Names

Andrew Sellars

Follow this and additional works at: https://scholarship.law.bu.edu/faculty_scholarship

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



The In Rem Forfeiture of Copyright-Infringing Domain Names

Andy Sellars*

1. Desperate Times, Novel Measures

Last year the United States began an operation to take down websites allegedly dealing in counterfeit goods and copyright-infringing material. Agents with the Immigration and Customs Enforcement division of the Department of Homeland Security (“ICE”) constructively removed these websites from the Internet through an *in rem* civil forfeiture action against their respective domain names, showing probable cause that the domain names constituted “property” used to infringe copyright.¹ In the enforcement sweep, named “Operation In Our Sites,” ICE agents obtained warrants ordering operators of website domain name registries to transfer ownership of the target domain names to the United States.² As a result, people attempting to visit these websites are rerouted to a government website declaring that the websites were “seized.”³ The owners of these websites did not have an opportunity to step forward and defend their sites before their domain names are taken, nor did ICE agents have to show that the operators themselves committed copyright infringement.⁴

This is a desperate remedy for desperate times. The “filesharing wars” of the past decade have led to a system of piracy where the websites storing and distributing infringing files on the Internet are detached from the websites that tell the public of the existence and location of such files, an attempt to evade many of the doctrines of secondary liability for infringement.⁵ To make

* J.D. Candidate 2011, The George Washington University Law School. Submitted for consideration in the 2011 Marcus B. Finnegan Prize Competition, sponsored by the law firm of Finnegan, Henderson, Farabow, Garrett & Dunner, LLP. Originally drafted for Prof. Dawn Nunziato’s Digital Copyright Seminar at GWU. Thanks to Prof. Nunziato and my peers in that class of substantive feedback. This work is available under a Creative Commons Attribution-Noncommercial 3.0 US License. For license terms, see <http://creativecommons.org/licenses/by-nc/3.0/us/>.

¹ See *infra* notes 68–70 and accompanying text.

² U.S. INTELLECTUAL PROPERTY ENFORCEMENT COORDINATOR, 2010 U.S. INTELLECTUAL PROPERTY ENFORCEMENT COORDINATOR ANNUAL REPORT ON INTELLECTUAL PROPERTY ENFORCEMENT 4 (Feb. 2011), available at http://www.whitehouse.gov/sites/default/files/omb/IPEC/ipec_annual_report_feb2011.pdf [hereinafter IPEC 2010 ANNUAL REPORT].

³ See *infra* notes 75–78 and accompanying text.

⁴ See *infra* notes 38–51 and accompanying text.

⁵ See *infra* notes 11–20 and accompanying text.

matters worse, it has become harder to enforce copyright law on the Internet, as centers of infringing activity are increasingly located abroad.⁶ The United States can only punish those over which courts can assert jurisdiction. The reach of the Internet, on the other hand, is not so constrained; persons inside the United States may reach the infringing content without difficulty. Proceeding *in rem* over the website provides an expedient way for law enforcement to take websites off the Internet that they view as violating copyright law regardless of their physical location.

This expedience, however, comes at an overwhelming cost to free speech. The websites seized are not mere archives of infringing works. In fact, most of the the websites seized thus far do not store the allegedly infringing content at all.⁷ Instead, they are discussion forums, chat rooms, blogs, and other forms of traditional, democratic speech.⁸ Such speech traditionally receives far stronger protection against its restraint. The websites may be enjoined for violations of copyright law consistent with the First Amendment, but currently no court fairly assesses the merits of such a claim before the websites are removed. This violates the procedural requirements placed over all other areas of expressive speech seized in the name of a content-based restriction, such as defamation or obscenity.⁹

Furthermore, proceeding *ex parte* against websites offering content that may or may not infringe copyright disrupts the cooperative spirit demanded by Congress in the online arena. The Digital Millennium Copyright Act (“DMCA”) indicates a preference by Congress to have content owners and web service providers communicate and cooperate when removing infringing content in some circumstances, such as when websites link to infringing content.¹⁰ Operation In Our Sites disrupts this cooperative system. To simply fall back to the notice-and-takedown process of the DMCA, though, would be an incomplete solution. There are times — such as when the website

⁶ See U.S. INTELLECTUAL PROPERTY ENFORCEMENT COORDINATOR, 2010 JOINT STRATEGIC PLAN ON INTELLECTUAL PROPERTY ENFORCEMENT 14 (June 2010), available at http://www.whitehouse.gov/sites/default/files/omb/assets/intellectualproperty/intellectualproperty_strategic_plan.pdf [hereinafter JOINT STRATEGIC PLAN].

⁷ See *infra* notes 79–86 and accompanying text.

⁸ See *id.*

⁹ See *infra* notes 108–127 and accompanying text.

¹⁰ See *infra* notes 159–163 and accompanying text.

operators are located internationally, unknowable, or deliberate scofflaws — where tactics such as *in rem* seizure may be needed.

Finally, there is substantial doubt that this enforcement tactic will work at all. Early evidence from the seizures already conducted indicates that most of the websites are back to their former popularity under different domain names. Furthermore, targeting the Internet domain name system used to route traffic on the Internet may lead some to setup competing domain name systems, which would undercut the fundamental architecture of the Internet.

Given these problems, it is doubtful that Operation In Our Sites should continue at all. However, if the government is insistent in using civil forfeiture of domain names as an enforcement tactic, certain safeguards must be imposed to conform with the First Amendment, to comply with the policy of cooperativeness indicated by Congress in the DMCA, and to improve overall efficacy. With respect to the First Amendment, the law should impose procedural safeguards akin to those used in obscenity cases to ensure that protected free speech is not overly swept up in the name of seizing unlawful, infringing speech. For the sake of preserving the general cooperative spirit of the DMCA, the law should be limited to specific cases where the notice-and-takedown process will not work, specifically, by requiring law enforcement to attempt *in personam* jurisdiction before seizing the content *in rem*. Finally, given the dubious odds of success and danger to Internet architecture by proceeding *in rem*, forfeiture of domain names should be used only in highly limited circumstances, where some extrinsic motivation suggests that seizing a domain name will actually take the website offline.

Part Two of this Paper gives some background on the efforts to combat filesharing online and the civil forfeiture remedy employed in this case. Part Three explains the seizures conducted in Operation In Our Sites in detail, and highlights some of the initial public responses. Finally, Part Four explains the issues with these seizures and ways in which courts and legislators could cure these infirmities.

2. Background

Copyright owners and those who share copyrighted files on the Internet have been locked in a decade long back-and-forth. The earliest websites making music available online were traditional websites placing files

on a central server.¹¹ The music industry closed those websites down rather easily.¹² Napster responded by decentralizing infringement, leaving the content on users' computers while still controlling a common server to direct traffic.¹³ The music industry persuaded the Ninth Circuit to find Napster contributorily liable due to their knowledge and control over infringing conduct.¹⁴ Aimster tried to create an architecture where encryption would make it impossible to know of infringing activity directly.¹⁵ The music industry successfully argued that this was a form of willful blindness, and the Seventh Circuit extended liability.¹⁶ Morpheus and Grokster relied on decentralized architecture to evade knowledge, creating a nodal system of users and superusers.¹⁷ The industries persuaded the Supreme Court to adopt an "inducement" theory of secondary liability to take these sites down.¹⁸ Filesharers responded by keeping the technology distinct from the filesharing activity, using protocols like BitTorrent and "cyberlocker" websites that do not engage in any direct filesharing services.¹⁹ Industries have responded by suing websites that create search indices for these decentralized files.²⁰ The litigation is ongoing.

Congress has provided substantive and procedural support for the content industries. Two recent laws are most relevant to this discussion. The first, the Artists' Rights and Theft Prevention Act ("ART Act"), passed within the larger Family Entertainment and Copyright Act of 2005, listed a new, specific offense to the criminal copyright infringement section: "making

¹¹ See Tim Wu, *When Code Isn't Law*, 89 VA. L. REV. 679, 727.

¹² See, e.g., *UMG Recordings, Inc. v. MP3.com, Inc.*, 92 F. Supp. 2d 349, 352–53 (S.D.N.Y. 2000).

¹³ Wu, *supra* note 11, at 728–29.

¹⁴ See *A&M Records, Inc. v. Napster, Inc.*, 239 F.3d 1004, 1020 (9th Cir. 2001).

¹⁵ See *In re Aimster Copyright Litigation*, 334 F.3d 643, 650–51 (7th Cir. 2003).

¹⁶ *Id.* at 650.

¹⁷ *MGM Studios Inc. v. Grokster, Ltd.*, 545 U.S. 913, 921 (2005).

¹⁸ *Id.* at 936–37.

¹⁹ See, e.g., *Columbia Pictures Indus., Inc. v. Fung*, No. CV 06-5578, 2009 WL 6355911 at *2 (C.D. Cal. Dec. 21, 2009). A "cyberlocker" website is a general name for a series of websites that allow for storage and retrieval of large-size files that may not be transmittable through other means. See Verified Complaint ¶ 8, *United States v. 7 Domain Names*, 10 cv 9203 (S.D.N.Y. filed Dec. 9, 2010) [hereinafter TVShack.net Complaint].

²⁰ See *Fung*, 2009 WL 6355911 at *19.

available” for download works that are “intended for commercial distribution.”²¹ This is targeted toward the activities of filesharers that may not have been prohibited by then-existing copyright law.²²

Second, in 2008 Congress passed the Prioritizing Resources and Organization for Intellectual Property Act (“PRO-IP Act”).²³ The PRO-IP Act made several changes to copyright law, including increased penalties for infringement and a new office within the Executive Office of the President dedicated to intellectual property, the Intellectual Property Enforcement Coordinator (“IPEC”).²⁴ The law further sought to unify and strengthen the seizure and forfeiture remedies against goods that infringed copyright or trademark law.²⁵ In so doing, the law greatly expanded the scope of the rarely-used civil forfeiture copyright remedy, opening the door for the domain name seizures that followed.²⁶

As forfeiture is rarely seen in the area of copyright law, it is worth exploring this remedy in greater detail.

²¹ Family Entertainment and Copyright Act of 2005, Pub. L. No. 109-9, § 102, 119 Stat. 218, 220 (codified in 18 U.S.C. § 2319B).

²² See, e.g., *Capitol Records, Inc. v. Thomas*, 579 F. Supp. 2d 1210, 1218–19 (D. Minn. 2008) (“making available” recordings for download is not “distribution” as defined in § 106 of the Copyright Act).

²³ Prioritizing Resources and Organization for Intellectual Property Act of 2008, Pub. L. No. 110-403, 122 Stat. 4256; see 4-15 NIMMER ON COPYRIGHT § 15.07[A] (2010).

²⁴ See 4-15 NIMMER ON COPYRIGHT § 15.07 (2010); Grace Pyun, *The 2008 PRO-IP Act: The Inadequacy of the Property Paradigm in Criminal Intellectual Property Law and its Effect on Prosecutorial Boundaries*, 19 DEPAUL J. ART, TECH., & INTELL. PROP. L. 335, 356 (2009).

²⁵ 4-15 NIMMER ON COPYRIGHT § 15.07. The seizure of counterfeit goods under trademark law has seen an expansion over the past several years, see Pyun, *supra* note 24, at 365–73, but has been a frequently-used aspect of trademark law for a longer period of time, see ROGER E. SCHECHTER & JOHN R. THOMAS, *INTELLECTUAL PROPERTY* § 29.6 (2003). While commentators raise alarm with increasing *ex parte* and *in rem* attempts to seize goods, the free speech and copyright policy questions raised in the web domain context do not directly apply in the area of trademark. For more on these concerns, see Steven N. Baker & Matthew Lee Fesak, *Who Cares About the Counterfeiters? How the Fight Against Counterfeiting Has Become an In Rem Process*, 83 ST. JOHN’S L. REV. 735 (2009); Jules D. Zalon, *Ex Parte Seizure Orders: Don’t Kill the Goose That Laid This Golden Egg!*, 23 COLUM.-VLA J.L. & ARTS 181 (1999). Discussions of domain name seizures as applied in the trademark context are beyond the scope of this Paper.

²⁶ See *infra* notes 68–78 and accompanying text.

2.1 Civil Forfeiture, Generally

Forfeiture laws concern the confiscation of property that is implicated in criminal activity.²⁷ Until the turn of the last century civil forfeiture in the United States was limited to the courts of admiralty.²⁸ In many admiralty disputes the person responsible for the action would be unknown or likely to flee.²⁹ It thus became expedient and convenient to proceed *in rem* against property itself, as if the property was the bad actor.³⁰ Later cases expanded the doctrine to tax evasion and bootleg liquor in the Prohibition era,³¹ and more recently the assets and finances of organized crime and drug cartels.³²

The efficiency of forfeiture laws can be demonstrated by how often the government simply takes custody of the relevant property without charging any person with a crime.³³ The government need only show probable cause that a connection exists between the property and the proscribed crime.³⁴ A wide range of evidence, including hearsay and other evidence usually unavailable at civil trial, can be used to establish this cause.³⁵ Once shown, the burden shifts to the owner of the property to establish by a preponderance of the evidence that the property was in fact unconnected to the crime.³⁶ In the

²⁷ LEONARD W. LEVY, *A LICENSE TO STEAL: THE FORFEITURE OF PROPERTY* ix (1996). The laws at issue in this note all concern the *in rem* proceedings civil forfeiture. Criminal forfeiture, which is conducted via *in personam* proceedings, is of a different history and character, and substantively outside the scope of this paper. *See generally id.* at 21–30.

²⁸ *See id.* at 39–45.

²⁹ *Id.* at 42–43.

³⁰ *Id.* at 43. A second theory for justifying actions taken against vessels themselves comes from Justice Holmes, who wrote of the inherent personality assigned to ships above all other inanimate objects. OLIVER WENDELL HOLMES, JR., *THE COMMON LAW* 26–27 (Dover Publications ed. 1991) (“It is only by supposing the ship to have been treated as if endowed with personality, that the arbitrary seeming peculiarities of the maritime law can be made intelligible....”)

³¹ LEVY, *supra* note 27, at 57–61; Baker & Fesak, *supra* note 25, at 735–38.

³² LEVY, *supra* note 27, at 62–70.

³³ *See id.* at 120.

³⁴ *Id.* at 48; *see* United States v. One Sharp Photocopier, 771 F. Supp. 980, 983 (D. Minn. 1991). Probable cause is determined using a flexible, totality-of-the-circumstances test. Illinois v. Gates, 462 U.S. 213, 238 (1983).

³⁵ *See, e.g.*, United States v. All Funds on Deposit in Any Accounts Maintained at Merrill Lynch, 801 F. Supp. 984, 990 (E.D.N.Y. 1992); *One Sharp Photocopier*, 771 F. Supp. at 983.

³⁶ LEVY, *supra* note 27, at 48; *One Sharp Photocopier*, 771 F. Supp. at 983.

words of Professor Leonard Levy, “[c]ivil forfeiture remains ... swift and cheap — and pretty much a sure thing.”³⁷

It is unsurprising to learn that the forfeiture doctrine has many critics, its history is with abuses.³⁸ Questions frequently arise regarding use of improper reward schemes, disproportionate use against minorities, the extremely limited defense for innocent owners of property, and the general inability of forfeiture to actually interdict or deter the crimes they are designed to combat.³⁹

2.2 Civil Forfeiture In Copyright

Civil forfeiture existed in copyright law before the enactment of the PRO-IP Act, but was limited in scope to the seizure of criminally-infringing copies and “all plates, molds, masters, tapes, film negatives, or other articles by means of which [infringing copies] may be reproduced, and all electronic, mechanical, or other devices for manufacturing, reproducing, or assembling such copies or records....”⁴⁰ Few cases using the old law were reported.⁴¹

The PRO-IP changes forfeiture law dramatically. The newly created Section 2323 of Title 18 establishes that articles “the making or trafficking of which are prohibited” by a series of intellectual property laws — including criminal copyright infringement,⁴² trafficking in counterfeit goods or labels falsely identifying copyrighted works as genuine,⁴³ and unauthorized

³⁷ LEVY, *supra* note 27, at 124.

³⁸ See *Calero-Toledo v. Pearson Yacht Leasing Co.*, 416 U.S. 663 (1974) (upholding forfeiture of a rented yacht under Puerto Rico law, after the lessees were caught with small amounts of marijuana on board); LEVY, *supra* note 27, at 2–6 (describing, *inter alia*, the attempted forfeiture of the *Atlantis II*, an \$80 million oceanographic research vessel, due to one crew member’s possession of one one-hundredth of an ounce of marijuana).

³⁹ See generally LEVY, *supra* note 27, at 134–42, 148–55, 161–76.

⁴⁰ 17 U.S.C. § 509(a) (repealed 2008).

⁴¹ In one case, a district court upheld the forfeiture of a photocopier after it was used to create infringing software manuals, which were bundled and sold with counterfeit software. *United States v. One Sharp Photocopier*, 771 F Supp. 980, 984–85 (D. Minn. 1991). In another, the Ninth Circuit denied use of § 509 to seize allegedly obscene materials. *Jartech, Inc. v. Clancy*, 666 F.2d 403, 408 (9th Cir. 1982). In a third, the First Circuit noted that § 509 is only available in criminal cases. *Gamma Audio & Video, Inc. v. Ean-Chea*, 11 F.3d 1106, 1113 (1st Cir. 1993).

⁴² See 17 U.S.C. § 506; 18 U.S.C. § 2319.

⁴³ See 18 U.S.C. §§ 2318(a)(1)(A), 2320.

recordings of live music performances or films being shown in theaters⁴⁴— are subject to forfeiture.⁴⁵ So is “any property used, or intended to be used, in any manner or part to commit or facilitate the commission of” the same crimes,⁴⁶ and “any property constituting or derived from the proceeds obtained directly or indirectly as a result of the commission of” the same.⁴⁷

The expansiveness of this change should not go unnoticed. Used most broadly, the old law would only allow the seizure of goods directly involved in the making process, the same scope authorized in the seizures conducted pursuant to an *in personam* copyright case.⁴⁸ The recent changes to copyright law have expanded the scope of both substantive criminal law and the civil forfeiture remedy, allowing for a seizure over “any property used” to commit or facilitate a wide array of crimes.⁴⁹ These crimes cover not only large-scale counterfeiters but a variety of common, though prohibited, activities.⁵⁰ Using these statutes, law enforcement agents could, in theory, seize a computer used to email an unreleased album to a friend (an activity many young adults do), or a cell phone used to tape part of a live musical performance (a frequent

⁴⁴ See §§ 2319A, 2319B.

⁴⁵ § 2323(a)(1)(A).

⁴⁶ § 2323(a)(1)(B).

⁴⁷ § 2323(a)(1)(C). The congressional record on this expansion is scant and cryptic. One of the only comments on the expanded forfeiture provision comes from a statement before the Senate, where Senator Patrick Leahy said that the bill “improves and harmonizes the forfeiture provisions in copyright and counterfeiting cases.” *Statement on Introduced Bills and Joint Resolutions*, U.S. SENATE, 154 CONG. REC. S7280-01 (July 24, 2008).

⁴⁸ Compare 17 U.S.C. § 509 (repealed 2008) with 17 U.S.C. § 503.

⁴⁹ 18 U.S.C. § 2323(a)(1)(B).

⁵⁰ 4-15 NIMMER ON COPYRIGHT § 15.01[2].

habit of concert-goers), or the profits derived from an artist whose fame began with an unlicensed cover of a song distributed online.⁵¹

The expansive nature of section 2323, particularly as it applies to websites, is central to appreciating the concerns around Operation in Our Sites. Before exploring these cases, however, one must understand the basic architecture of the Internet.

2.3 Internet Architecture⁵²

The Internet is a decentralized system.⁵³ It is, at heart, simply a network of computers that send files to each other.⁵⁴ In order to do so computers on the Internet are assigned numerical addresses (“IP addresses”).⁵⁵ Those seeking to host content on the Internet place that data on a computer connected to the Internet (a “server,” usually owned and operated by a professional service).⁵⁶ Once connected, any computer can then enter that server’s IP address into their browser to receive content.

⁵¹ In fact, a colorable argument exists for the seizure and forfeiture all profits earned by pop star Justin Bieber. Bieber began his career by posting videos on popular video website YouTube. See Desiree Adib, *Teen Pop Star Justin Bieber Discovered on YouTube*, ABC NEWS (Nov. 14, 1999), <http://abcnews.go.com/GMA/Weekend/teen-pop-star-justin-bieber-discovered-youtube/story?id=9068403>. One of the videos he posted was an unauthorized cover of a Chris Brown song, likely a violation of copyright law. See *With You*, YOUTUBE, <http://www.youtube.com/watch?v=eQOFRZ1wNLw> (last viewed March 28, 2011). If Bieber subjectively knew that the law proscribed this conduct, this would be a willful violation of copyright. See, e.g., *United States v. Moran*, 757 F. Supp. 1046, 1051 (D. Neb. 1991). One can stipulate that this was done for financial gain — the kind of financial gain that getting signed to a major record label can bring. This would escalate this action into a criminal violation of copyright. See 17 U.S.C. § 506(a)(1)(A). Given this, section 2323 states that any proceeds or property directly or indirectly attributable to this infringement could be forfeit. 18 U.S.C. § 2323. If indeed this video was the reason he was signed to a major label, and Bieber knew the video infringed copyright, this would put all of his subsequent property and proceeds into jeopardy.

⁵² Computer science professionals will note that this is a simplification of Internet architecture, done for purposes of demonstrating the issue at the heart of this Paper.

⁵³ MATTHEW MACDONALD, *CREATING A WEB SITE* 53 (2d ed. 2009).

⁵⁴ *Id.* at 9–14.

⁵⁵ Orin Kerr, *The Problem of Perspective in Internet Law*, 91 GEO. L. J. 357, 363 (2003).

⁵⁶ MACDONALD, *supra* note 53, at 13–14.

IP addresses appear as a string of numbers.⁵⁷ To require Internet users to remember such numbers would be quite annoying to those users. Instead, the Internet has a human-readable language resting on top of IP addresses, called the Domain Name System (“DNS”).⁵⁸ This system uses Uniform Resource Locators (“URLs,” such as “http://www.website.com/”) to convey information about the content the browser is trying to reach.⁵⁹ While humans read this code quite easily, computers cannot, and thus systems must be in place for computers to “resolve” human-readable URLs into computer-readable IP addresses.⁶⁰

In order for this system to work the same URL typed into two different computers would need to resolve to the same IP address. An organization called the Internet Corporation for Assigned Names and Numbers (“ICANN”) was formed to standardize this system.⁶¹ ICANN operates a system whereby a single company called a “registry” is responsible for managing the domain names within a given top level domain (a “TLD,” for example, “.com,” “.net,” or “.org”).⁶² These registries then contract with a series of different “registrars,” who offer domain names within that TLD to the public (who, when they register websites, are referred to as “registrants”).⁶³ Registrants are free to decide what IP address that domain name will resolve to, and they can change that address at any time.⁶⁴

⁵⁷ Kerr, *supra* note 55, at 363. The current system is running out of space, and is about to expand to a new system with addresses using a slightly longer alphanumeric string. See generally Iljitsch van Beijnum, *Everything You Need to Know About IPv6*, ARS TECHNICA (March 7, 2007), <http://arstechnica.com/hardware/news/2007/03/IPv6.ars/>.

⁵⁸ Kerr, *supra* note 55, at 363.

⁵⁹ For example, the URL “http://www.website.com/files/page.html” conveys that the data is accessible using the HyperText Transport Protocol (“HTTP”), is located at the domain registered in the “.com” registry for “website,” is in the “files” path at that address, and in the file “page.html.” See MACDONALD, *supra* note 53, at 54–55.

⁶⁰ Barry M. Leiner et al., *A Brief History of the Internet*, INTERNET SOCIETY, <http://www.isoc.org/internet/history/brief.shtml> (last viewed March 27, 2011).

⁶¹ *What Does ICANN Do?*, ICANN (last updated Aug. 13, 2010), <http://icann.org/en/participate/what-icann-do.html>.

⁶² *Id.* The system operates slightly differently for “country code TLDs” – the domain addresses ending with a two letter code signifying a given country, but not in a way that significantly alters the analysis of this Paper. See *id.*

⁶³ *Id.*

⁶⁴ MACDONALD, *supra* note 53, at 64–65. These changes typically take a couple of days to promulgate to the various DNS servers. See ICANN, *supra* note 61.

Such description may seem needlessly technical, but it is vitally important to understanding the current copyright enforcement tactic employed by the United States. To the lay user Internet traffic seems to move seamlessly, but on the backend a wide array of transactions take place to provide us that experience.⁶⁵ And, for reasons noted below, forfeiture remedies based on the lay user's "internal" perspective of how the Internet works may not be effective due to realities in the "external" systems governing Internet traffic.⁶⁶

3. Operation In Our Sites

The government has made clear that a large focus of intellectual property enforcement will be targeted toward the Internet.⁶⁷ To that end, ICE has developed a tactic of using the new civil forfeiture powers from the PRO-IP Act to disrupt and interdict the online distribution of copyright-infringing material and counterfeit goods, executed in Operation In Our Sites.⁶⁸ ICE Director John Morton calls the effort a "first-of-its-kind aggressive and strategic offensive that methodically targets counterfeiters on the Internet who pirate any copyrighted material."⁶⁹ The operation's objective is to seize domain names selling counterfeit goods and providing access to infringing content.⁷⁰

Three waves of seizures have been executed under this operation, and in all cases the copyright-related seizures were vastly outnumbered by seizures for trademark-related offenses.⁷¹ The operation began in June of 2010, when

⁶⁵ See Jonathan Zittrain, *Internet Points of Control*, 44 B.C. L. REV. 653, 658 (2003).

⁶⁶ This "internal" and "external" nomenclature comes from Kerr, *supra* note 55, at 359–61. For more on its shortcomings in this case, see *infra* notes 186–189 and accompanying text.

⁶⁷ JOINT STRATEGIC PLAN, *supra* note 6, at 5.

⁶⁸ See IPEC 2010 ANNUAL REPORT, *supra* note 2, at 21.

⁶⁹ *Id.* at appx. 3.

⁷⁰ *Id.* at 6. It may be difficult to comprehend how the remedy in these cases—the forced alteration of a website registry—can be called a "seizure," when nothing is taken from any party, and nothing is held in custody by the United States. This is only a problem, however, if one uses the plain meaning of the word "seizure." If one considers "seizure" as a term of art meaning "some meaningful interference with an individual's possessory interests in ... property," *United States v. Jacobsen*, 466 U.S. 109, 113 (1984), the "seizure" in these cases is understandable. There are claimants in each case who would claim a possessory interest in the domain names at issue, and by exercising control over their routing the United States can be seen as interfering with that possessory interest.

⁷¹ See IPEC 2010 ANNUAL REPORT, *supra* note 2, at 14–15.

an ICE agent filed in the Southern District of New York for the forfeiture of nine domain names that were allegedly linking to copies of movies that were only legally accessible in theaters.⁷² In November 2010, an ICE agent filed in the Central District of California for the seizure of five copyright-infringing websites as part of a larger sweep of sites selling physical copies of counterfeit goods.⁷³ Finally, in late January 2011, an ICE agent applied for a warrant to seize ten domain names in the Southern District of New York targeting the unauthorized “streaming,” or Internet transmission, of live sporting telecasts.⁷⁴

While each wave of the operation is distinct, they share a common trait in the remedy. The targets of Operation In Our Sites are websites with “.net,” “.com,” and “.org” TLDs.⁷⁵ These are all TLDs with registries located inside the United States.⁷⁶ In order effectuate the seizure of the domain name, the affidavits request that a magistrate order the registries for these TLDs to restrain and lock the target domain names, transfer right and title to those

⁷² “Operation In Our Sites” Targets Internet Movie Pirates, U.S. IMMIGRATION AND CUSTOMS ENFORCEMENT (June 30, 2010), <http://www.ice.gov/news/releases/1006/100630losangeles.htm>; see TVShack.net Complaint, *supra* note 19, at ¶¶ 12, 18–19, 23–24, 28–29, 33–34, 38–39, 43–44. The factual descriptions of the cases that follow are largely based on the assertions made by federal agents in applications for seizure warrants, criminal complaints, and other accusatory documents. In many cases the veracity of these claims has not been adjudicated. Indeed, some are hotly contested. See Mike Masnick, *Full Homeland Security Affidavit to Seize Domain Names Riddled with Technical & Legal Errors*, TECHDIRT (Dec. 21, 2010), <http://www.techdirt.com/articles/20101221/00420012354/full-homeland-security-affidavit-to-seize-domains-riddled-with-technical-legal-errors.shtml>. For purposes of this discussion, however, the factual allegations in these cases are treated as true.

⁷³ IPEC 2010 ANNUAL REPORT, *supra* note 2, at 42. The seizures were timed to take down these websites immediately before “Black Friday,” traditionally the largest retail shopping day of the year. *Id.*

⁷⁴ Affidavit in Support of Application for Seizure Warrant ¶ 7, *United States v. 10 Domain Names*, 11 Mag 262 (S.D.N.Y. filed Jan. 31, 2011) [hereinafter HQ-Streams.com Affidavit]. Not likely by chance, the seizure was conducted less than a week before the Super Bowl. Chad Bray, *Sports Websites Seized in Crackdown on Illegal Streaming*, WALL ST. JOURNAL (Feb. 2, 2011), <http://online.wsj.com/article/SB10001424052748703960804576120263283106584.html>.

⁷⁵ See TVShack.net Complaint, *supra* note 19; HQ-Streams.com Affidavit, *supra* note 74; Application and Affidavit for Seizure Warrant, *In re 5 Domain Names*, No. 10-2822M (C.D. Cal. filed Nov. 17, 2010) [hereinafter RapGodfathers.com Affidavit].

⁷⁶ See *Registry Listing*, ICANN, <http://www.icann.org/en/registries/listing.html> (last viewed April 10, 2011). ICE also used this forfeiture remedy against one website whose top level domain is the country code for Tuvalu, “.tv.” TVShack.net Complaint, *supra* note 19. However, because the American company Verisign administers this domain name, the registry for the “.tv” TLD is still located in reach of United States courts. See VERISIGN.TV, <http://www.verisign.tv/>.

domain names to the United States, and have those domain names resolve to a particular IP address owned by ICE.⁷⁷ On the server located at ICE’s designated IP address is a website that posts an image declaring that the domain has been seized by ICE pursuant to a warrant, and reminding the reader that it is unlawful to reproduce copyrighted material without authorization.⁷⁸

The target websites — tvshack.net, movies-links.tv, zml.com, now-movies.com, thepiratecity.org, planetmovies.com, filespump.com, rapgodfathers.com, torrent-finder.com, rmx4u.com, dajaz1.com, onsmash.com, hq-streams.com, atdhe.net, firstrow.net, channelsurfing.net, ilemi.com, and rojadirecta.org — were alleged to be unlawful “linking” websites.⁷⁹ This is a term used to define websites that contain links to files stored on pure storage or “cyberlocker” websites.⁸⁰ One of the websites was a cyberlocker itself.⁸¹ The actual servers containing the websites are located both domestically and abroad, specifically in Colorado, Florida, Illinois, Texas, Utah, and Virginia, as well as the Bahamas, Canada, the Czech Republic, Germany, Luxembourg, the Netherlands, Sweden and the United Kingdom.⁸²

The websites were largely centered around discussion forums and chat rooms, but the content of those fora often included links to infringing music, movies, live broadcasts and/or software stored on third-party websites.⁸³ Several of the websites were also monetized with advertising.⁸⁴ The

⁷⁷ HQ-Streams.com Affidavit, *supra* note 74, ¶¶ 48–49; RapGodfathers.com Affidavit, *supra* note 75, at ¶¶ 102–04.

⁷⁸ *See, e.g.*, HQ-Streams.com Affidavit, *supra* note 74, at Attachment A. At the time of this writing, a visit to any of the seized domains named below will present a user with this website.

⁷⁹ TVShack.net Complaint, *supra* note 19, at ¶ 9; RapGodfathers.com Affidavit, *supra* note 75, at ¶¶ 36, 57, 75, 87, 97; HQ-Streams.com Affidavit, *supra* note 74, at ¶ 13. Some of the websites had alternative domain names that were seized along with the primary domains listed above. *See* HQ-Streams.com Affidavit, *supra* note 74.

⁸⁰ TVShack.net Complaint, *supra* note 19, at ¶ 9.

⁸¹ *Id.* at ¶ 22.

⁸² *Id.* at ¶¶ 11, 16, 21, 26, 31, 36, 41; RapGodfathers.com Affidavit, *supra* note 75, at ¶¶ 36, 57, 75, 87, 97; HQ-Streams.com Affidavit, *supra* note 74, at ¶¶ 16, 23, 27, 30, 33, 40.

⁸³ RapGodfathers.com Affidavit, *supra* note 75, at ¶¶ 17, 42, 58; HQ-Streams.com Affidavit, *supra* note 74, at ¶ 13.

⁸⁴ *See* RapGodfathers.com Affidavit, *supra* note 75, at ¶¶ 17, 53–54, 94.

complaints and affidavits declare these websites as “property used or intended to be used to willfully infringe a copyright,” and thus subject to forfeiture under section 2323.⁸⁵ The justification of many of these is that they “made available” works that were not yet available to the public.⁸⁶

In the online community, the response to these seizures was predictably apoplectic.⁸⁷ Members of Congress, including Senator Ron Wyden and Representative Zoe Lofgren, have publicly questioned the propriety and authority of ICE and IPEC to engage in this form enforcement.⁸⁸ The seizures happen to come at a time when Congress is contemplating allowing highly similar *in rem* procedures against websites “dedicated to infringing activity,” in the proposed Combating Online Infringements and Counterfeits Act.⁸⁹ To make matters worse, a related ICE domain name seizure recently took down 84,000 innocent websites by

⁸⁵ TVShack.net Complaint, *supra* note 19, at ¶ 4; RapGodfathers.com Affidavit, *supra* note 75, at ¶ 106; HQ-Streams.com Affidavit, *supra* note 74, at ¶ 5.

⁸⁶ 17 U.S.C. § 506(a)(1)(C). *See, e.g.*, RapGodfathers.com Affidavit, *supra* note 75, at ¶¶ 18, 26, 31, 37, 79, 91.

⁸⁷ *See, e.g.*, Mike Masnick, *ICE Boss: It's Okay to Ignore the Constitution if It's to Protect Companies*, TECHDIRT (Feb. 28, 2011), <http://www.techdirt.com/articles/20110228/11122813301/ice-boss-its-okay-to-ignore-constitution-if-its-to-protect-companies.shtml>; Corynne McSherry, *ICE Seizures Raising New Free Speech Concerns*, ELECTRONIC FRONTIER FOUNDATION (Feb. 16, 2011), <https://www.eff.org/deeplinks/2011/02/ice-seizures-raising-new-speech-concerns>; Michael Arceneaux, *Opinion: Whose Internet Is It Anyway?*, AOL NEWS (Dec. 2, 2010), <http://www.aolnews.com/2010/12/02/opinion-whose-internet-is-it-anyway/>; David Makarewicz, *5 Reasons Why the US Domain Seizures Are Unconstitutional*, TORRENTFREAK (March 12, 2011); *but see* Terry Hart, *Domain Name Seizures Don't Violate First Amendment*, COPYHYPE (Jan. 17, 2011), <http://www.copyhype.com/2011/01/domain-name-seizures-dont-violate-first-amendment/>.

⁸⁸ Mike Masnick, *Rep. Lofgren Challenges IP Czar on Legality of Domain Seizures*, TECHDIRT (March 4, 2011), <http://www.techdirt.com/articles/20110304/01390113359/rep-lofgren-challenges-ip-czar-legality-domain-seizures.shtml>; Jennifer Martinez, *Ron Wyden Questions Sports Site Take-Down*, POLITICO (Feb. 3, 2011), <http://www.politico.com/news/stories/0211/48804.html>.

⁸⁹ *See* Combating Online Infringement and Counterfeits Act, S. 3804, 111th Cong. (2010); *see also* Grant Gross, *Senator Threatens to Block Online Copyright Bill*, PC WORLD (Nov. 19, 2010 11:40AM), http://www.pcworld.com/businesscenter/article/211162/senator_threatens_to_block_online_copyright_bill.html (noting efforts by Senator Wyden to block the bill in the last session of Congress).

accident.⁹⁰ Countless theories have been port forth as to why these seizures are unlawful, unconstitutional, or simply improper.⁹¹

4. Present Risks and Possible Solutions in Domain Name Forfeiture

This Paper focuses on three specific problems inherent in the tactics employed by Operation In Our Sites, and ways in which those problems can be avoided and cured. For reasons noted below, procedural safeguards need to be implemented to protect against the improper seizure of constitutionally protected speech. Furthermore, due to the potential conflict of this remedy with the cooperation encouraged by Congress in the DMCA “safe harbor” provisions for linking websites, this tactic should only be used when it is not possible to contact the operator of the website through an *in personam* process. Finally, due to the dubious efficacy and potential risk inherent in adopting this tactic, civil forfeiture of websites should be limited to atypical and extreme cases. Each of these concerns and remedies is discussed in turn.

4.1 Free Speech Concerns and Procedural Safeguards

The harm to free speech implicated by the actions in Operation In Our Sites is facially apparent. The websites targeted contained a great deal of legitimate, non-infringing speech, including chat rooms, discussion forums, and blog posts.⁹² This is the kind of speech that the First Amendment traditionally protects with vigor. The websites were taken down without a chance for the owners of the websites to respond, and upon only probable

⁹⁰ Nate Anderson, *Silicon Valley Congresswoman: Web Seizures Trample Due Process (And Break the Law)*, ARS TECHNICA (March 14, 2011), <http://arstechnica.com/tech-policy/news/2011/03/ars-interviews-rep-zoe-lofgren.ars>.

⁹¹ For example, it is unclear why ICE should have the authority for enforcing domain name traffic originating from domestic web servers. See JOINT STRATEGIC PLAN, *supra* note 6, at 26–28. Also, the seizures raise important questions of due process and opportunity to be heard, as do most actions regarding the remote seizure of material. See generally Mark A. Lemley & Eugene Volokh, *Freedom of Speech and Injunctions in Intellectual Property Cases*, 48 DUKE L.J. 147, 164–65 (1998); FED. R. CIV. P. 65 advisory committee’s note (1966) (“In view of the possibly drastic consequences of a temporary restraining order, the opposition should be heard, if feasible, before the order is granted.”). Finally, the breadth of the scope of civil and criminal forfeiture raises a panoply of due process and fairness concerns, both inside and outside the copyright context. See 18 U.S.C. § 2323(a)(1)(B), (C). All of these concerns further the argument for ceasing application of civil forfeiture to websites, but are substantively outside the scope of this article. For more, see Makarewicz, *supra* note 87.

⁹² See *supra* notes 76–86 and accompanying text.

cause of infringement demonstrated. Under traditional doctrines of free speech law, this would not be tolerated.⁹³

It is well established that speech found to infringe copyright — that is, speech that is identical or “substantially similar” to another’s currently protected expression — is not saved from liability by the First Amendment.⁹⁴ But it is equally clear that expression that does not infringe copyright deserves full First Amendment protection like any other speech. Despite the litany of arguments that are raised to make copyright a “special case” different from other forms of expression,⁹⁵ actions taken in the name of copyright enforcement are subject to First Amendment scrutiny.⁹⁶ That the actions may (indeed, almost always do) satisfy such scrutiny should not remove this antecedent step.

And the question here is not whether substantive free speech law would save the websites from copyright liability. It is clear that it would not, if adjudicated as infringing.⁹⁷ Instead, the question is whether the *in rem* seizure of pure speech, done because it *may* be infringing, violates the *procedural* safeguards instituted by the First Amendment.⁹⁸ Here, entire websites consisting of pure expression were removed, presumably because some of the speech encouraged viewers to follow links to third-party websites and commit

⁹³ See *infra* notes 107–127 and accompanying text.

⁹⁴ *Eldred v. Ashcroft*, 537 U.S. 186, 221 (2003); Lemley & Volokh, *supra* note 91, at 167.

⁹⁵ Popular variations include that copyright law protects a “property” right, that it involves private and not government enforcement, that it covers kinds of speech not relevant to democracy and self-governance, that copyright furthers free speech, and that copyright is an enumerated power within Article I of the Constitution. See Lemley & Volokh, *supra* note 91, at 182–97 (raising and rejecting these claims and others).

⁹⁶ *Eldred*, 537 U.S. at 221 (“We recognize that the D.C. Circuit spoke too broadly when it declared copyrights ‘categorically immune from challenges under the First Amendment.’” (quoting *Eldred v. Reno*, 239 F.3d 372, 375 (D.C. Cir. 2001))).

⁹⁷ See *Eldred*, 537 U.S. at 221.

⁹⁸ See Henry P. Monaghan, *First Amendment “Due Process”*, 83 HARV. L. REV. 518, 537–38 (1970).

copyright infringement.⁹⁹ Direct copyright infringement was not being conducted on these websites at all; it was instead the cyberlockers that reproduced and distributed the content.¹⁰⁰ If the speech is adjudicated to be “inducing” under that secondary liability theory the speech is likely enjoined consistent with the First Amendment.¹⁰¹ If it is not so found, it is constitutionally protected free speech.¹⁰² And at this moment no court has actually turned to the merits of this claim and determined if it is indeed unlawfully inducing. Instead, a magistrate judge determined that there was a sufficient probability that it may be infringing, and used that alone to take the website down. Courts would not tolerate such a cursory review in all other areas of free speech law.¹⁰³

The First Amendment embodies certain procedural safeguards to help prevent free speech from being accidentally silenced while unprotected speech is enjoined. An analogy to obscenity doctrine can provide useful guidance. Like infringing speech, obscene speech is unprotected by the First Amendment.¹⁰⁴ The determination of whether a work is obscene also depends entirely upon an examination of its content, requiring application of

⁹⁹ The claimed justification for seizure is the forfeiture provision in 18 U.S.C. § 2323. *See, e.g.*, TVShack.net Complaint, *supra* note 19, at ¶ 49. This law states that property “used, or intended to be used, in any manner or part to commit or facilitate the commission” of copyright infringement is subject to forfeiture. 18 U.S.C. § 2323(a)(1)(B). The theory of infringement here could be based on either the “making available” crime of 17 U.S.C. § 506 (a)(1)(C), or the inducement liability developed by the Supreme Court in *MGM Studios, Inc. v. Grokster, Ltd.*, 545 U.S. 913, 936–37. For nearly all of these websites it would be incorrect to state that the website “made available” the work, as unrelated, third-party websites were actually placing the work on the internet. *See supra* notes 79–80. Therefore, the only way in which the websites here would be “used” to facilitate copyright infringement would be through words on the website indicating where infringing content is located online, be it in plain English or in the hybrid language of hyperlinks.

¹⁰⁰ *See, e.g.*, HQ-Streams.com Affidavit, *supra* note 74, at ¶ 13.

¹⁰¹ *See Eldred*, 537 U.S. at 221 (2003); *Grokster*, 545 U.S. at 936–37.

¹⁰² *See United States v. Stevens*, 130 S. Ct. 1577, 1584 (2010) (restrictions upon speech based on content are only tolerated in a few narrowly limited classes of speech).

¹⁰³ *See Center for Democracy & Technology v. Pappert*, 337 F. Supp. 2d 606, 657 (E.D. Pa. 2004) (a scheme that allowed a district attorney to disable access to websites based on a probable cause finding that they constituted child pornography was procedurally inadequate and thus a prior restraint).

¹⁰⁴ *See generally Miller v. California*, 413 U.S. 15, 23–24 (1973).

a legal test to specific facts.¹⁰⁵ And in both cases the difference between protected and unprotected speech can sometimes be a “dim line.”¹⁰⁶

Courts are quite sensitive about the precarious line between proscribable speech and protected speech, and are very hostile against government efforts that engage in “prior restraint.”¹⁰⁷ Prior restraints are considered the “most serious and least tolerable infringement on First Amendment rights,”¹⁰⁸ and bear a “heavy presumption” against validity.¹⁰⁹ Any effort to remove speech from circulation before the speech is adjudicated as unlawful can work an unconstitutional prior restraint, even when imposed after the speech is published.¹¹⁰

To that end, courts have recognized that seizure of expressive works requires special procedural considerations.¹¹¹ For example, seizure of allegedly obscene materials always requires a warrant.¹¹² Agents applying for warrants must state more than “conclusory allegations” that an observed work is unlawful by reason of obscenity.¹¹³ That said, warrants need not show more than standard probable cause to justify seizure.¹¹⁴

The scope of seizures is also highly significant. The Supreme Court’s jurisprudence indicates different treatment for seizures of one or a few copies of a work, done for the preservation of evidence, and seizures conducted as a

¹⁰⁵ *See id.* at 24–25.

¹⁰⁶ *See Bantam Books, Inc. v. Sullivan*, 372 U.S. 58, 66 (1963) (“[T]he Fourteenth Amendment requires that regulation by the States of obscenity conform to procedures that will ensure against the curtailment of constitutionally protected expression, which is often separated from obscenity only by a dim and uncertain line.”).

¹⁰⁷ *See Simon & Schuster, Inc. v. Members of the N.Y. State Crime Victims Bd.*, 502 U.S. 105, 127 (Kennedy, J., concurring); Lemley & Volokh, *supra* note 91, at 171.

¹⁰⁸ *Neb. Press Ass’n v. Stuart*, 427 U.S. 539, 559 (1976).

¹⁰⁹ *New York Times Co. v. United States (Pentagon Papers)*, 403 U.S. 713, 714 (1971) (per curiam).

¹¹⁰ *Bantam Books*, 372 U.S. at 70 (finding a prior restraint even though the restriction was imposed after the work was published).

¹¹¹ *See Fort Wayne Books, Inc. v. Indiana*, 489 U.S. 46, 62–63 (1989); *New York v. P.J. Video, Inc.*, 475 U.S. 868, 873 (1986).

¹¹² *Roaden v. Kentucky*, 413 U.S. 496, 503–05 (1973).

¹¹³ *Lee Art Theatre, Inc. v. Virginia*, 392 U.S. 636, 637 (1968) (per curiam).

¹¹⁴ *New York v. P.J. Video, Inc.*, 475 U.S. 868, 875 (1986). On remand of this case the New York Court of Appeals held that a heightened form of probable cause was required under state constitutional law. *See People v. P.J. Video, Inc.*, 501 N.E.2d 556, 564–65 (N.Y. 1986).

means to impound and destroy all copies of an expressive work.¹¹⁵ The former is generally permissible, provided that the court promptly determine the legality of the work.¹¹⁶ But seizures that have the effect of taking the work entirely out of circulation have been rejected repeatedly, absent full adjudication of illegality.¹¹⁷

The Supreme Court examined the free speech implications of forfeiture proceedings in *Alexander v. United States*.¹¹⁸ Following a jury verdict against a criminal defendant for obscenity, the district court in *Alexander* granted the government's motion for forfeiture of the defendant's business assets and real estate, including many non-obscene expressive works.¹¹⁹ The Supreme Court found the seizure to be subsequent punishment for unlawful conduct, thus not warranting prior restraint analysis.¹²⁰ However, the Court expressly distinguished criminal forfeiture of property *after* the adjudication of guilt from seizure of expressive works *before* full adjudication of their unprotected status.¹²¹ "[T]he seizure was not premature" in this case, the court reasoned, "because the Government established beyond a reasonable doubt the basis for the forfeiture."¹²²

Notwithstanding this consistent disfavor of prior restraints, there is one particular area of obscenity jurisprudence that allows for governmental restraint of speech before full adjudication.¹²³ In *Freedman v. Maryland* the Supreme Court addressed the growing practice in the states to create boards of review for motion pictures that may contain obscenity.¹²⁴ While striking Maryland's system for such review, the Court indicated that a system could

¹¹⁵ *Heller v. New York*, 413 U.S. 483, 491–92 (1973).

¹¹⁶ *Heller*, 413 U.S. 492–93.

¹¹⁷ See *A Quantity of Books v. Kansas*, 378 U.S. 205, 210 (1964) (plurality opinion); *Marcus v. Search Warrants*, 367 U.S. 717, 731–33 (1961).

¹¹⁸ 509 U.S. 544, 547 (1993).

¹¹⁹ *Id.* at 548 n.1.

¹²⁰ *Id.* at 550–551. The case was remanded on Eighth Amendment grounds. *Id.* at 559.

¹²¹ *Id.* at 551–52.

¹²² *Id.* at 552; see also *Adult Video Ass'n v. Reno*, 41 F.3d 503, 504–05 (9th Cir. 1994) (upholding RICO seizure of obscene material after adjudication of guilt in a criminal proceeding, but not a pre-trial seizure).

¹²³ See *Freedman v. Maryland*, 380 U.S. 51 (1965); Lemley & Volokh, *supra* note 91, at 179.

¹²⁴ See *Freedman*, 380 U.S. at 57.

exist, provided four procedural safeguards are provided.¹²⁵ Specifically, (1) the burden of proving that the speech is unprotected must rest on the government, (2) the state's administrative determination that the speech is unprotected must not be final, (3) any restriction must "be limited to preservation of the status quo for the shortest fixed period compatible with sound judicial resolution," and (4) final judicial decision must be reached promptly.¹²⁶ Absent these carefully crafted safeguards, courts will not tolerate a prior restraint of speech.¹²⁷

Needless to say, these safeguards were not followed in Operation In Our Sites. The seizures here were not done to preserve evidence, as nothing tangible was taken into custody, and it would be illogical to claim that there was any risk that a defendant would "flee" with their domain name and thus deprive the court of evidence.¹²⁸ This seizure instead took the website out of circulation entirely, at least for a time.¹²⁹ No administrative proceeding with the safeguards of *Freedman* was present. Instead, a single federal agent made a probable-cause level statement to a magistrate judge, who ruled *ex parte*. In striking contrast to the careful process required when seizing expressive works in the doctrine of obscenity, the seizures conducted in Operation in Our Sites show the bare minimum of process. This turns First Amendment due process on its head; it takes down speech on the basis of its content (to wit, that it is infringing content or induces others to infringe copyright) before an adversarial proceeding determines if the speech is in fact unlawful.

This is not to argue, however, that *in rem* seizures are incurably unconstitutional. There exists an easy to fix this law's present infirmity. Congress could avoid the problem of prior restraint by imposing the

¹²⁵ *Id.* at 58–59.

¹²⁶ *Id.*

¹²⁷ *See id.* at 58.

¹²⁸ Makarewicz, *supra* note 87.

¹²⁹ *Cf.* *Mortgage Specialists, Inc. v. Implode-Explode Heavy Indus., Inc.*, 999 A.2d 184, 196 (N.H. 2010) (finding an injunction preventing the republication of online content to be an unlawful prior restraint).

procedural safeguards of *Freedman* into the domain name seizure process.¹³⁰ This would require an adversarial hearing where the government bears the burden of proving that the website can be seized under the doctrine of copyright law.¹³¹ If this is done in an administrative court it must be subject to judicial review.¹³² A final judicial determination must be reached “promptly,” though the Supreme Court has not specifically stated how promptly, other than to indicate that it is a matter of days, not months.¹³³ Finally, because seizure of the website would take the potentially protected work entirely out of circulation, and preservation of the evidence related to the website can be done through less intrusive means,¹³⁴ a law enforcement agent should satisfy the burdens here (at least up to the point of a first administrative determination) *before* the website is taken offline.

To execute a forfeiture proceeding under this process, therefore, a law enforcement agent could bring a complaint articulating the justification for seizure to a United States district court or expedited agency appealable to a district court. The adjudicatory body or law enforcement agent would then exercise best efforts to give notice to the owner of the domain name at issue, in order to create an adversarial proceeding. The government would then bear the burden of proving that the website infringed copyright, and the owner of the website would be able to assert any valid copyright defenses or dispute this proof. Judicial resolution would be reached promptly, and the website would be either forfeit or restored. If forfeitable, any appropriate restitution can then be levied against the owner of the website for the infringement occurring

¹³⁰ Professors Mark Lemley and Eugene Volokh argue that similar application of *Freedman* can be imposed over preliminary injunctions in copyright. Lemley & Volokh, *supra* note 91, at 180. Nevertheless, they are skeptical of such a system as a matter of First Amendment law. *See id.* at 214. They also do not support such a system over “time-sensitive” works. *See id.* at 215.

¹³¹ *Freedman*, 380 U.S. at 58; *see* Carroll v. Princess Anne Cnty., 393 U.S. 175 (1968) (*ex parte* orders are not allowed where “no showing is made that it is impossible to serve or notify the opposing parties”).

¹³² *Freedman*, 380 U.S. at 58–59.

¹³³ *See* United States v. 37 Photographs, 402 U.S. 363, 370–72 (1971) (plurality opinion) (interpreting the Tariff Act as requiring limits of 14 days for commencement at 60 days for completion of forfeiture proceeding, in order to avoid unconstitutionality, noting that processes taking “three, four, and even seven months” would be “clearly inconsistent with the concern for promptness”).

¹³⁴ For example, a law enforcement agent may take screenshots or archive copies of the website as it exists relatively easily. *See* HQ-Streams.com Affidavit, *supra* note 74, at Ex. A–F (providing such screenshots).

while the forfeiture process was ongoing.¹³⁵ By simply imposing the same respect for potentially infringing speech that is imposed for potentially obscene speech, the First Amendment issue is avoided.

Opponents will no doubt raise the frequency of injunctions in copyright cases as demonstration that we should not be so concerned with prior restraint. It is true that injunctions before and after adjudication of infringement have been part of intellectual property since inception.¹³⁶ Preliminary injunctions in *inter partes* cases are quite common.¹³⁷ On occasion a plaintiff may even obtain an *ex parte* restraining order prior to trial, following Rule 65 of the Federal Rules of Civil Procedure, allowing seizure before the opponent even has an opportunity to respond.¹³⁸

But even preliminary injunctive relief in an *inter partes* proceeding involves a more careful process than the probable cause used for *in rem* civil forfeiture.¹³⁹ The Supreme Court recently noted (albeit in dicta) that injunctions in copyright must follow “traditional equitable considerations,” which presupposes at least an adversarial proceeding and balancing of interests before injunction.¹⁴⁰ Furthermore, there has been increasing concern about this remedy’s harm to free speech,¹⁴¹ and courts are hostile to this remedy when the action seems to be an attempt to silence speech disfavored by the copyright owner.¹⁴²

Critics also argue that First Amendment analysis is inappropriate because the websites were not seized because of their expressive content, but because they are “property” used to facilitate crimes.¹⁴³ This has intuitive

¹³⁵ See 18 U.S.C. § 2323(c).

¹³⁶ Lemley & Volokh, *supra* note 91, at 151–54. That said, they were used somewhat sparingly until the twentieth century. See *id.* at 154–58.

¹³⁷ *Id.* at 158–59.

¹³⁸ *Id.* at 164.

¹³⁹ Though, as Professors Lemley and Volokh argue, it may not provide enough procedure to survive constitutional scrutiny. See *id.* at 210.

¹⁴⁰ eBay Inc. v. MercExchange, LLC, 547 U.S. 388, 392–93 (2006).

¹⁴¹ See *Salinger v. Colting*, 607 F.3d 68, 82 (2d Cir. 2010) (noting that the public interest in receiving information may outweigh issuance of a copyright injunction). The court in *Salinger* expressly avoided addressing the argument that copyright injunctions are an invalid prior restraint of speech. See *id.* at 76.

¹⁴² See *Ty, Inc. v. Publ’ns Int’l Ltd.*, 292 F.3d 512, 521 (7th Cir. 2002) (finding fair use when the plaintiff “want[ed] to suppress criticism of its product”).

¹⁴³ Hart, *supra* note 87.

appeal. After all, we do not use the First Amendment to stop the closure of a bar that violates liquor laws, even though bars are often places where members of the public gather to debate the issues of the day.

The problem with this argument is it unfairly characterizes the law at issue. Copyright forfeiture is not a content-neutral law allowing for the seizure of any property used in crime. The law providing for forfeiture in copyright cases expressly incorporates substantive copyright law.¹⁴⁴ Copyright itself is a content-based form of regulation: it determines the legality or illegality of speech on the basis of how the speech is expressed.¹⁴⁵ To equate content-based laws with content-neutral laws does not conform with First Amendment doctrine.¹⁴⁶ These websites were not seized here because their domain name offended copyright. It was the *speech* on the website, allegedly telling people where and how to find infringing content, that was the crux of the forfeiture. The object of the domain name seizure was to constructively remove this offending speech. The analysis of illegality here begins and ends with an examination of the speech for its content.

A final argument against free speech safeguards is that waiting for adjudication will be too costly, as with some forms of infringement (such as the live streaming of television broadcasts, or the distribution of movies online while the films being shown in theaters) the “damage is done” within minutes or days of the infringing act.¹⁴⁷

¹⁴⁴ See 18 U.S.C. § 2323 (allowing for forfeiture of articles that violate 17 U.S.C. § 506).

¹⁴⁵ Copyright laws may be motivated by a general interest, but they do restrict speech on the basis of content, albeit without reference to a particular viewpoint or subject matter. See *Cardtoons, L.C. v. Major League Baseball Players Ass’n*, 95 F.3d 959, 971 (10th Cir. 1996) (“Intellectual property, unlike real estate, includes the words, images, and sounds that we use to communicate, and ‘we cannot indulge in the facile assumption that one can forbid particular words without also running a substantial risk of suppressing ideas in the process.’” (quoting *Cohen v. California*, 403 U.S. 15, 26 (1971))); DAVID LANGE & H. JEFFERSON POWELL, *NO LAW: INTELLECTUAL PROPERTY IN THE IMAGE OF AN ABSOLUTE FIRST AMENDMENT* 372-73 (2009) (“Defining content is at the center of [copyright]. ... Copyright, which subsists only in expression, can never be merely content neutral”); Lemley & Volokh, *supra* note 91, at 165–66 (“Copyright law restricts speech: it restricts you from writing, painting, publicly performing, or otherwise communicating what you please. If your speech copies ours, and if the copyright uses our “expression,” not merely our ideas or facts that we have uncovered, the speech can be enjoined and punished, civilly and sometimes criminally.”).

¹⁴⁶ See *Turner Broad. Sys., Inc. v. FCC*, 512 U.S. 622, 640–41 (1994).

¹⁴⁷ See *HQ-Streams.com Affidavit*, *supra* note 74, at ¶¶ 10, 12.

This argument ignores the very reason why courts are so hesitant to engage in prior restraint in the first place. The same argument could be raised for defamatory speech, speech that could threaten national security, or speech that incites others to violence, and yet we do not tolerate prophylactic injunctions in those cases.¹⁴⁸ In fact, it is time-sensitivity that cautions against removing speech, even temporarily, in this case.¹⁴⁹ Imagine a website operating around the time of a presidential debate, hosting a live feed of a copyrighted telecast of the debate alongside a chat room or similar forum. Visitors to the website could view the coverage of the debate and discuss it coterminously, engaging in quintessential free expression. Yet, under the logic of the warrants used in Operation In Our Sites such websites are subject to forfeiture without any consideration of this expression or its time-sensitivity. Indeed, one warrant uses the live streaming of news broadcasts as evidence supporting justification of a seizure.¹⁵⁰ Once seizure is granted, the website would disappear for weeks or months while the forfeiture proceeding continues. The seizure of the domain name would thus have a direct, timely impact on a channel of free expression, one that could not be cured by subsequent reinstating of the website after adjudication on the merits.¹⁵¹ If instead the website was subject to the procedural safeguards above, including an expedited review process like in *Freedman* test, the free speech harms can be avoided.

4.2 Copyright Policy and *In Personam* Exhaustion

The underlying claim in most of the cases in Operation In Our Sites is that the website violated copyright law by linking to other websites that stored infringing content. The argument is easy to follow: linking to material can allow users to quickly locate content.¹⁵² If users then download content from

¹⁴⁸ Lemley & Volokh, *supra* note 91, at 176; *See* New York Times Co. v. United States (*Pentagon Papers*), 403 U.S. 713, 714 (per curiam) (leaks of confidential military documents).

¹⁴⁹ *See* *Pentagon Papers*, 403 U.S. at 715 (1971) (Black, J., concurring) (“[E]very moment’s continuance of the injunctions against these newspapers amounts to a flagrant, indefensible, and continuing violation of the First Amendment.”).

¹⁵⁰ HQ-Streams.com Affidavit, *supra* note 74, at ¶¶ 21, 26.

¹⁵¹ *See* Lemley & Volokh, *supra* note 91, at 198–99.

¹⁵² *See* RapGodfathers.com Affidavit, *supra* note 75, at ¶ 12.

these links they may not buy a legitimate copy.¹⁵³ This deprives the author of revenue, and thus the incentive for authors to create and disseminate creative works is reduced.

But copyright does not protect against all potential economic harms faced by authors.¹⁵⁴ The rights of copyright are specifically enumerated,¹⁵⁵ and courts are surprisingly unclear as to whether linking itself implicates one of these enumerated rights.¹⁵⁶ Of course, this analysis is largely limited to direct liability for infringement. If this linking was done by the owner of the website to induce others to infringe copyright they would be liable under the theory of *Grokster*.¹⁵⁷ And if the websites knew of the infringing quality of the links they would be found liable under a contributory infringement theory.¹⁵⁸

It is likely that few cases arise regarding linking because there exists a “safe harbor” for content linking created by the Digital Millennium Copyright Act (“DMCA”).¹⁵⁹ This creates a liability shield for websites providing “information location tools” such as hyperlinks, provided that the website neither has actual knowledge that specific material is infringing nor is aware of facts “from which infringing activity is apparent.”¹⁶⁰ The website must also comply with the “notice-and-takedown” process of the DMCA, removing

¹⁵³ How many may or may not do so, of course, is uncertain. *See generally* Felix Oberholzer & Koleman Strumpf, *The Effect of File Sharing on Record Sales: An Empirical Analysis* (2004), available at http://www.unc.edu/~cigar/papers/FileSharing_March2004.pdf; Daniel Gross, *Does a Free Download Equal a Lost Sale?*, N.Y. TIMES (Nov. 21, 2004), <http://www.nytimes.com/2004/11/21/business/yourmoney/21view.html>.

¹⁵⁴ *See* Feist Publ'ns, Inc. v. Rural Tel. Serv. Co., 499 U.S. 340, 364 (1991).

¹⁵⁵ *See* 17 U.S.C. § 106.

¹⁵⁶ *Compare* Batesville Servs. v. Funeral Depot, Inc., No. 02-cv-01011, 2004 WL 2750253 at *12 (S.D. Ind. Nov. 10, 2004) (owner of linking website liable when owner placed content on second website and linked to it); *Intellectual Reserve v. Utah Lighthouse Ministry*, 75 F. Supp. 2d 1290, 1294–95 (D. Utah 1999) (likelihood of success on contributory infringement claim, when defendant informed users where infringing content can be located on his website); *with* *Perfect 10, Inc. v. Amazon.com, Inc.*, 508 F.3d 1146, 1160–61 (9th Cir. 2007) (“framing” a website using in-line linking is not infringement); *Online Policy Grp. v. Diebold, Inc.*, 337 F. Supp. 2d 1195, 1202 n.12 (N.D. Cal. 2004) (hyperlinking is not per se direct infringement, but may bring rise to contributory liability in some cases); *Arista Records v. MP3Board, Inc.*, No. 00-civ-4660, 2002 WL 1997918 at *3 (S.D.N.Y. Aug. 29, 2002) (same).

¹⁵⁷ *MGM Studios, Inc. v. Grokster, Ltd.*, 545 U.S. 913, 936–37 (2005).

¹⁵⁸ *See* *Fonovisa, Inc. v. Cherry Auction, Inc.*, 76 F.3d 259, 264 (9th Cir. 1996).

¹⁵⁹ 17 U.S.C. § 512(d).

¹⁶⁰ § 512(d)(1). The “apparent” standard, often called a “red flag” standard, is set at a very high bar. *See* *Viacom Int'l, Inc. v. YouTube, Inc.*, 718 F. Supp. 2d 514, 520–21 (S.D.N.Y. 2010) (discussing identical language in § 512(c)).

content upon written notice from a copyright owner that a link contains infringing material.¹⁶¹

This is not just coincidence or legislative good fortune for websites that frequently link to content that may be infringing. The safe harbors of the DMCA are a legislative expression of a desire to foster cooperation between online service providers and copyright owners.¹⁶² The legislative history around the safe harbor indicates that the provision is “intended to promote the development of information location tools generally, and Internet directories ... in particular.”¹⁶³ The statute mandates a bargain between these two groups: the websites will have a designated person to receive complaints and respond expeditiously to remove infringing links, and in exchange the copyright owners will not sue the websites for infringement through their linking.

This spirit of cooperation vanishes when enforcement moves from an *inter partes* to an *ex parte* remedy. The copyright owner is no longer encouraged to reach out to the website owner. Instead, they will persuade ICE to file a seizure warrant to take down the disputed websites. The website owner now has no chance to expeditiously right the perceived wrong. Instead she must come forward in court and dispute the criminality of the seized domain name.¹⁶⁴ A nervous website owner would probably prefer letting that website die out and starting a new one elsewhere. This induces evasion. It is therefore unsurprising that these websites have the feel of criminality; the law treated them as criminals. The forfeiture provisions of the PRO-IP Act undercut the cooperative spirit of the DMCA, when applied against websites.

Before passing judgment on the websites at issue here, it is worth noting that many were demonstrating the cooperative spirit lauded above. An affiliate with one website claims they took great efforts to comply with the

¹⁶¹ § 512(d)(3). Although not directly stated, it appears as though the notice-and-takedown process would require the service to register an agent to receive such notice with the Copyright Office. *See* § 512(c)(2).

¹⁶² *See* S. REP. NO. 105-190, at 40 (1998).

¹⁶³ *Id.* at 49.

¹⁶⁴ FED. R. CIV. P. Supplemental Admiralty and Maritime Rule G(5) (detailing the procedure for interested parties to dispute forfeiture).

DMCA.¹⁶⁵ The operator of another seized website claims it received several of its linked tracks from record company employees, indicating that the content owners and website operators were already in communication.¹⁶⁶ Another affidavit mentions that a user on one site was banned after posting link to download the Adobe Photoshop program.¹⁶⁷ A few of the websites included disclaimers stating that they were compliant with copyright law.¹⁶⁸ One website even encouraged people to purchase a leaked album on iTunes, in order to receive bonus tracks.¹⁶⁹

What's more, there is evidence in the affidavits here that the notice-and-takedown process of the DMCA were working. An ICE agent notes in one affidavit that he attempted to follow a link to reach a cyberlocker website only to find that the file was "no longer available."¹⁷⁰ This happened again when the agent tried to download a Chris Brown album, only to find that the file was removed from the linked cyberlocker site due to a copyright claim from the International Federation of the Phonographic Industry.¹⁷¹

While the cooperative spirit of the DMCA may be demonstrated in some of these cases, it of course does not follow that all of these websites are operating in good faith vis-à-vis copyright law. The November 17th affidavit goes to great lengths to tie the infringing content linked to the website with administrators of the target website, suggesting inducement liability.¹⁷² Furthermore, while the affidavits mention in passing the contact information

¹⁶⁵ See *A Message to All Artists*, BYC PROMOTION (Nov. 26, 2010), <http://www.bycpromo.com/2010/11/message-to-all-artists-must-read.html> (quoting an anonymous source affiliated with rapgodfathers.com as saying, "[w]e always removed links connected with any DMCA requests").

¹⁶⁶ Nate Anderson, *Undue Process: How Uncle Sam Seized BitTorrent Domain Names*, ARS TECHNICA (Dec. 20, 2010), <http://arstechnica.com/tech-policy/news/2010/12/busting-bittorrent.ars>.

¹⁶⁷ RadGodfathers.com Affidavit, *supra* note 75, at ¶¶ 66–67. It is unclear whether the agent was able to download a copy of Photoshop from the link that the banned user posted. In any event, the agent was able to download the program from another link. *Id.* ¶ 66.

¹⁶⁸ See, e.g., HQ-Streams.com Affidavit, *supra* note 74, at ¶ 21; RapGodfathers.com Affidavit, *supra* note 75, at ¶¶ 17, 37.

¹⁶⁹ RapGodfathers.com Affidavit, *supra* note 75, at ¶ 88. Of course, the distribution of the "leaked" album would still be infringement, but the encouragement to purchase a legitimate copy seems quite genuine.

¹⁷⁰ *Id.* at ¶ 25.

¹⁷¹ *Id.* at ¶ 79.

¹⁷² See *id.* at ¶¶ 19 n.6, 21, 45, 72, 78, 88.

for several of the operators of these websites,¹⁷³ others are located abroad and may not be inclined to respond to the demands of a foreign copyright owner. Requiring strict compliance to the notice-and-takedown process would not be effective against those determined to infringe copyrights, or those outside American jurisdiction.

But copyright law need not chose between the lesser of two evils here. The law can generally encourage a cooperative atmosphere in solving online infringement problems, while simultaneously providing an *in rem* remedy when necessary. Such a balance already exists in the area of trademark law. The Anti-Cybersquatting Consumer Protection Act (“ACPA”) guards against those who occupy the domain names of trademarks with a bad faith intent to profit by providing a civil *in rem* remedy for trademark owners.¹⁷⁴ Before exercising an *in rem* remedy, however, the owner must demonstrate that she cannot assert *in personam* jurisdiction over the person who would be the defendant, or “through due diligence was not able to find a person who would have been a defendant”¹⁷⁵ This encourages proceeding in trademark disputes *inter partes*, but allows for an *in rem* option should such efforts fail.¹⁷⁶

To apply such a system here would generally support the cooperative spirit of the DMCA by requiring *inter partes* communication, but would still preserve a remedy for such circumstances where an *inter partes* remedy is not possible. Requiring law enforcement to proceed against the person behind a website instead of the website itself, at least initially, could lead to amicable

¹⁷³ See *id.* at ¶ 78.

¹⁷⁴ 15 U.S.C. § 1125(d)(2).

¹⁷⁵ § 1125(d)(2)(A)(ii).

¹⁷⁶ *Lucent Techs., Inc. v. LucentSucks.com*, 95 F. Supp. 2d 528, 534 (E.D. Va. 2000) (*In rem* actions are “a last resort where *in personam* jurisdiction is impossible, because the domain name registrant is foreign or anonymous”). Under ACPA, plaintiffs must bring a claim in the district in which the domain name registrar or registry is located (which typically means the Eastern District of Virginia, where Verisign is located). 15 U.S.C. § 1125(d); see *Ford Motor Co. v. Greatdomains.com, Inc.*, 177 F. Supp. 2d 656, 657–58 (E.D. Mich. 2001). The forfeiture provisions governing Operation In Our Sites do not require this. See 18 U.S.C. § 2323 (18 U.S.C. § 981 governs procedure in copyright forfeiture); § 981(b)(3) (seizure warrants may be obtained in any jurisdiction authorized under 18 U.S.C. § 1355); § 1355(b)(1)(A) (forfeiture action may be brought in the district court “in which any acts or omissions giving rise to forfeiture occurred”). This Paper expresses no opinion as to whether the *in rem* actions here should be brought in a particular United States District Court, provided the court where the suit is brought satisfies general due process requirements in *in rem* actions. See *Shaffner v. Heitner*, 433 U.S. 186, 207 (1977) (basis for jurisdiction *in rem* must satisfy the “fair play and substantial justice” standard of *International Shoe Co. v. Washington*, 326 U.S. 310, 316 (1945)).

resolution of the issues at stake without employing the dramatic remedy of civil forfeiture.¹⁷⁷

The reason content owners or law enforcement would prefer not proceeding *in personam* is probably the greater expedience and lower standards of proof available when acting *in rem*.¹⁷⁸ That expedience, however, may come at the cost of efficacy. As noted below, many of these websites were able to evade the *in rem* remedy with little difficulty.¹⁷⁹ They would risk contempt of court to do so in an *inter partes* proceeding. Addressing these websites directly may also lead them to adopt voluntary additional protections for content owners, much like those YouTube adopted surrounding its infringement litigation with Viacom.¹⁸⁰ Too much is made of what is gained by proceeding *in rem*, and too little of what is lost.

One might also argue that the prosecutorial discretion of law enforcement could ensure that domain name forfeiture would be employed only in appropriate circumstances. The facts of these cases suggest otherwise. Many of the websites targeted in Operation In Our Sites are located on servers inside of the United States.¹⁸¹ One particular website, channelsurfing.net, reopened shortly after its domain was seized with a slightly different URL.¹⁸² It was only after the operator was contacted (which is a euphemistic way of saying “arrested”¹⁸³) that the website actually closed.¹⁸⁴ If ICE had simply gone to the person directly they could have saved

¹⁷⁷ Ideally, of course, these actions would be brought by the copyright owners themselves, as person-to-person negotiation would likely be far more productive than law-enforcement-agency-to-person negotiations. Nevertheless, ICE agents could act as a representative of a multitude of content owners and achieve the same effect.

¹⁷⁸ See *supra* notes 33–37 and accompanying text.

¹⁷⁹ See *infra* notes 186–189 and accompanying text.

¹⁸⁰ *Viacom Int’l, Inc. v. YouTube, Inc.*, 718 F. Supp. 2d 514, 527–28 (S.D.N.Y. 2010) (noting the three-strikes policy and “Claim Your Content” systems created by YouTube).

¹⁸¹ See *supra* note 82.

¹⁸² Phillip Barnard, *Wrestling Fans Left in the Dark After Several Streaming Websites Get Shut Down*, THE EXAMINER (Feb. 3, 2011), <http://www.examiner.com/pro-wrestling-in-houston/wrestling-fans-left-the-dark-after-several-streaming-websites-get-shut-down>. For more on this evasion tactic, see Part 4.3, *infra*.

¹⁸³ See Complaint, *United States v. McCarthy*, No 11-mj-521 (S.D.N.Y. filed Feb. 28, 2011).

¹⁸⁴ See David Farrell, *Update: Channelsurf.eu Down*, THE EXAMINER (March 18, 2011), <http://www.examiner.com/sitcom-in-national/update-channelsurf-eu-down-operating-out-of-new-site-as-owner-faces-arrest> (noting that channelsurf.eu, the replacement for channelsurfing.net closed shortly after McCarthy’s arrest).

this intermediate step. Similarly, rather than simply seize the domains of websites truly willing to cooperate under the DMCA, ICE agents could instruct the operators and the general public how to operate consistent with copyright law. Given the vastness of websites that host content on the Internet, an ounce of public education could be worth a pound of enforcement.

If the owner of the website chooses evasion over cooperation, then ICE could employ the *in rem* remedy. But to do so in all cases would subvert the policies of the DMCA and would not be as effective at deterring actual infringement on the Internet. For these reasons, Congress should adopt an *in personam* exhaustion requirement akin to the remedy in ACPA.

4.3 Practical Failure and Prosecutorial Caution

There exists a more fundamental problem with this enforcement tactic: it does not seem to be working. The remedy used by ICE in Operation In Our Sites does not actually interdict or disrupt the activities of these websites above a trivial level.¹⁸⁵ Rerouting a domain name system in the name of misdirecting those who would reach such sites to infringe copyright will not deter or disrupt those that are determined to continue such infringement. As they did with every previous legal hurdle in the filesharing wars, the filesharers have already found away around it.

The seizure warrants in these cases specifically target the domain names of allegedly infringing websites. As explained above, a domain name is simply an addressing system used to convert machine-readable IP addresses into English-language words to facilitate human communication around the Internet.¹⁸⁶ They are not attached to the actual servers hosting web content.¹⁸⁷ Accordingly, “seizing” the domain name will not disturb the web servers or their IP addresses. Operators are free to register their IP address with a new, different domain name registrar and obtain a new domain name, this time with a TLD registry located outside the reach of American courts. Many

¹⁸⁵ See *infra* notes 186–189 and accompanying text.

¹⁸⁶ See Section 2.3 *supra*.

¹⁸⁷ The IPEC Annual Report states that 90 domain names were seized, to one actual server. IPEC 2010 ANNUAL REPORT, *supra* note 2, at 21.

websites seized in Operation In Our Sites already have.¹⁸⁸ As a result, some websites were only down for a matter of hours, and some (anticipating such a move by the government) were never taken offline entirely.¹⁸⁹

Nevertheless, proponents of the seizures argue forcefully that the seizures do in fact disrupt the operation of these websites.¹⁹⁰ The facts do not bear that out.¹⁹¹ The ICE agents in Operation In Our Sites used website Alexa rankings in their affidavits to help demonstrate the relative popularity of these websites on the Internet.¹⁹² It is possible to compare these rankings to the present ranking of the replacement websites to gauge how effective these seizures actually were.

The results, for ICE, are embarrassing. It appears that some of the replacement websites are already more popular than the websites seized. For example, rapgodfathers.com was the 15,150th most popular website in the United States before seizure.¹⁹³ After moving to rapgodfathers.info its

¹⁸⁸ See, e.g., Jared Moya, *ICE Domain Seizures a Pointless Exercise*, ZEROPAID (Nov. 29, 2010), <http://www.zeropaid.com/news/91400/ice-domain-seizures-a-pointless-exercise/> (“2009jerseys.com is back as 2009jerseys.net, RapGodfathers.com is back as RapGodfathers.info, NFLJerseySupply.com is back as NFLJerseySupply.net, golfwholesale18.com is back as golfwholesale18.net, and torrent-finder.com is back as torrent-finder.info.”).

¹⁸⁹ Richard Abbott, *DNS Boondoggle: Why the COICA Has Already Failed*, BNA PATENT, TRADEMARK & COPYRIGHT LAW DAILY (March 4, 2011), http://news.bna.com/ptdm/display/story_list.adp?mode=ins&frag_id=19938267&prod=ptdm (noting that rojadirecta.com already had rojadirecta.es as a backup domain name at the time of seizure).

¹⁹⁰ See Terry Hart, *A Response to “Supporters of DHS Domain Name Seizures Undervalue Important Constitutional Protections”*, COPYHYPE (April 4, 2011), <http://www.copyhype.com/2011/04/a-response-to-supporters-of-dhs-domain-name-seizures-undervalue-important-constitutional-protections/>; Gautham Nagesh, *Film Industry Lauds Web Crackdown on Copyright Law Violators*, THE HILL (March 30, 2011), <http://thehill.com/blogs/hillicon-valley/technology/152601-film-industry-lauds-web-crackdown-on-violators-of-federal-copyright-law>.

¹⁹¹ Mike Masnick, *Are Homeland Security's Domain Seizures Actually Working? Doesn't Look Like It*, TECHDIRT (April 6, 2011), <http://www.techdirt.com/articles/20110403/21352913751/are-homeland-securitys-domain-seizures-actually-working-doesnt-look-like-it.shtml>.

¹⁹² See, e.g., RapGodfathers.com Affidavit, *supra* note 75, at ¶ 34; HQ-Streams.com Affidavit, *supra* note 74, at ¶¶ 22, 40. The Alexa company operates an algorithm to calculate the relative popularity of websites on the Internet. By way of spectrum comparison, Google, Facebook, and YouTube are the three most popular websites, CNN is presently ranked 52nd in the world, Bittorrent tracker site the Pirate Bay is 87th, commercial video site Hulu.com is 223rd, The Washington Post is 347th, political news aggregator The Drudge Report is 433rd, Wired Magazine is 659th, the official website of Major League Baseball is 1,056th, popular culture blog BoingBoing.net is 1,605th, the official website of *The Daily Show with Jon Stewart* is 3,898th, President Obama's whitehouse.gov is 4,434th, and legal gossip blog Above the Law is 30,408th. See ALEXA: THE WEB INFORMATION COMPANY, <http://www.alexa.com/> (last viewed March 14, 2011).

¹⁹³ RapGodfathers.com Affidavit, *supra* note 75, at ¶ 34.

popularity increased to 12,387th.¹⁹⁴ Onsmash.com was the 9,520th most popular website in the United States.¹⁹⁵ Its replacement, freeonsmash.com, eclipsed its predecessor and now is the 7,194th most popular.¹⁹⁶

Others are still less popular than their original websites, but are rapidly gaining popularity. Before being seized, the domain atdhe.net was the 664th most popular website in the world.¹⁹⁷ Atdhe.net's replacement website, atdhenet.tv, is already the 3,799th most popular website.¹⁹⁸ Seized domain rojadirecta.org was the 2,380th most popular website;¹⁹⁹ its replacement, rojadirecta.es, is presently the 3,351st.²⁰⁰

This should offend opponents of government wastefulness as much as critics of the underlying policy. To setup a new domain name is trivial. Websites can and will be back online in a matter of hours.²⁰¹ It is conceivable that a single instance of a seizure would lead the owner of a website to "get the point" and opt not to open a new domain name, but this is an unlikely possibility.

Given this, a critic may ask where the harm is in playing this game of legal Whac-A-Mole. If the websites are back up in a matter of hours or days, where is the harm to the website owners? Aside from the First Amendment problems inherent in even a temporary restraint of speech, and the greater efficacy possible when proceeding *in personam*, a legitimate website that is unfairly seized under a probable-cause *in rem* warrant would suffer a permanent harm to their reputation. The websites will bear the mark of

¹⁹⁴ *Rapgodfathers.info Site Info*, ALEXA, <http://www.alexa.com/siteinfo/rapgodfathers.info> (last viewed April 10, 2011).

¹⁹⁵ RapGodfathers.com Affidavit, *supra* note 75, at ¶ 96.

¹⁹⁶ *Freeonsmash.com Site Info*, ALEXA, <http://www.alexa.com/siteinfo/freeonsmash.com> (last viewed April 10, 2011).

¹⁹⁷ HQ-Streams.com Affidavit, *supra* note 74, at ¶ 22.

¹⁹⁸ *Atdhenet.tv Site Info*, ALEXA, <http://www.alexa.com/siteinfo/atdhenet.tv> (last viewed March 14, 2011).

¹⁹⁹ HQ-Streams.com Affidavit, *supra* note 74, at ¶ 40.

²⁰⁰ *Rojadirecta.es Site Info*, ALEXA, <http://www.alexa.com/siteinfo/rojadirecta.es> (last viewed March 14, 2011).

²⁰¹ See generally Ernesto Van Der Sar, *US Government's "Pirate" Domain Seizures Failed Miserably*, TorrentFreak (April 3, 2011), <http://torrentfreak.com/us-governments-pirate-domain-seizures-failed-miserably-110403/>

illegality and illegitimacy, which may not be deserved. One can easily picture a nascent YouTube swept into this enforcement tactic.²⁰²

This is not a speculative assertion. In a related enforcement sweep using a similar remedy, federal agents targeted the website mooo.com.²⁰³ This domain name did not represent just one website, however. It had 84,000 other websites located on subdomains, all of which were seized.²⁰⁴ In their place was a banner saying that the website had been seized for involvement with child pornography, which of course was completely false.²⁰⁵ Congresswoman Zoe Lofgren, outraged by this seizure, suggested the websites sue the Department of Homeland Security.²⁰⁶

Furthermore, there exists a remote but plausible possibility that this seizure would encourage others to create a rival domain name system to compete with the system instituted by ICANN. This would be devastating to the architecture of the Internet. Most people rely on the DNS instituted by ICANN, which standardizes the system to make sure that two people who type in the same domain name will receive the same IP address.²⁰⁷ This is nothing more than a default setting; if one wanted to point to a different DNS server than those instituted by their Internet service provider, one could configure a computer to do so.²⁰⁸ If the United States insists on continuing to target websites at the DNS level, increasing numbers of people may migrate to

²⁰² See *The COICA Internet Censorship and Copyright Bill*, ELECTRONIC FRONTIER FOUNDATION, <https://www.eff.org/coica> (last viewed April 9, 2011) (pondering such a possibility under the proposed COICA legislation).

²⁰³ Anderson, *supra* note 90.

²⁰⁴ Ernesto Van Der Sar, *U.S. Government Shuts Down 84,000 Websites*, TORRENTFREAK (Feb. 16, 2011), <http://torrentfreak.com/u-s-government-shuts-down-84000-websites-by-mistake-110216/>.

²⁰⁵ See Anderson, *supra* note 90.

²⁰⁶ *Id.*

²⁰⁷ ICANN, *supra* note 61. It is a bit of a simplification to say that most computers rely on the ICANN DNS servers. Technically, when a computer is attempting to resolve a domain name to an IP address it first checks the web browser to see if the website has been accessed recently, then the computer's operating system to see if there are superseding instructions, then potentially a local DNS server (located at a web router, for example), and then their Internet service provider's DNS Server, who in turn check the root servers operated by ICANN. Abbott, *supra* note 189.

²⁰⁸ To do so is quite easy. See *Google Public DNS*, GOOGLE, <https://code.google.com/speed/public-dns/> (last viewed April 10, 2011) (providing instructions to configure a computer to access Google's free DNS service).

an independent DNS system, beyond the reach of United States courts.²⁰⁹ Users could also instruct their computers to override DNS in certain instances (such as correcting the domain names rerouted through Operation In Our Sites), or simply start referring to websites by their numerical IP addresses.²¹⁰ All of this would undercut the reliability of DNS servers. The Internet simply cannot function if “www.website.com” points to two different places on two different computers, depending on which DNS server is used.

Given all of this, the best remedy may be for ICE to save its money and stop this enforcement tactic altogether. ICE Director John Morton has indicated, however, that he has no intention to do so.²¹¹ If ICE is insistent on employing this remedy, they should do so quite sparingly, and not when there exists a better way to target the website. There should be some extrinsic reason to believe that seizing a domain name will actually result in the website being taken offline.²¹² Otherwise, the law is engaged in a carnival game. It is highly unlikely that the tactic will actually result in less infringement.

5. Conclusion

It is clear that the Executive Branch of the United States is determined to increase online intellectual property enforcement in the coming years.²¹³ This is right and good, but tactics used in enforcement should not disrupt free speech or the values of copyright. Nor should they constitute an ineffective and wasteful use of government resources.

²⁰⁹ Abbott, *supra* note 189. OpenDNS is already a popular alternative to the standard DNS servers, offering malware protection, typo correction, and an advertised faster DNS cache. *OpenDNS Overview*, OPENDNS, <http://www.opendns.com/solutions/overview/> (last viewed April 10, 2011).

²¹⁰ Abbott, *supra* note 189. An example of the latter came after the registrar for the controversial website Wikileaks terminated its service. Users began referring to the website simply as “<http://213.251.145.96>.” Typing this into a web browser instructs the computer to skip the DNS lookup and go to the IP address directly. *See id.*; Alex Williams, *Wikileaks Loses its DNS Service*, READ WRITE WEB (Dec. 2, 2010), <http://www.readwriteweb.com/cloud/2010/12/wikileaks-loses-its-dns-servic.php>.

²¹¹ Ernesto Van Der Sar, “*Operation In Our Sites*” Will Continue Seizing Domains, TORRENTFREAK (April 7, 2011), <http://torrentfreak.com/operation-in-our-sites-will-continue-seizing-domains-110407/>.

²¹² Such reason is inherently fact specific, and up the speculation and imagination of law enforcement to employ effectively. Such consideration may be related to the spoken manifestations of a target defendant, the presence of an irreplaceable domain name, or the character and behavior of the target defendant.

²¹³ *See* IPEC 2010 ANNUAL REPORT, *supra* note 2, at 7 (“Law enforcement efforts have increased in the past year and will continue to do so.”).

Operation In Our Sites cannot continue in its present form. Its total disregard for the free speech issues at stake when seizing domain names violates the First Amendment, by ignoring the procedural safeguards the Supreme Court has found proper to protect that substantive right. Furthermore, it ignores the policy adopted by Congress at the outset of the Internet age, encouraging content owners and website providers to adopt a “notice-and-takedown” process that even the warrants used in Operation In Our Sites indicate seems to be working far better than civil forfeiture. Finally, the operation, and all of the money spent promoting and selling it to the public, has likely resulted in net-zero change to copyright piracy online. Filesharers figured away around the system within hours of the websites being seized.

If Operation In Our Sites is to continue, Congress, the courts, and law enforcement should employ a series of changes to correct these problems. The law should follow the procedural safeguards of First Amendment doctrine, employing the adversarial hearing and expedient adjudication standards of *Freedman v. Maryland* to civil forfeiture seizures of expressive content. Civil forfeiture should be employed only when it is not possible to reach the website operator using *in personam* jurisdiction. Finally, ICE should recognize that the system employed here has a low likelihood of success, absent some other extrinsic consideration, and should be used quite sparingly, if at all.