5-1-2013

Ice Under Fire: Impropriety of Domain Name Seizures

Shane Alexander McDougall

ICE UNDER FIRE: IMPROPRIETY OF DOMAIN NAME SEIZURES

I. INTRODUCTION

In recent years the United States Government has increased its effort to hamper online copyright infringement.[1] In a number of planned seizures, the Government has seized website domains that were found to have been hosting or linking to copyrighted material such as sports broadcasts, movies, and music.[2] The seizures have been made possible by statute, specifically the Pro-IP Act, which allows the government to seize property that is alleged to be infringing copyrights.[3] These seizures have been met with a significant amount of controversy for a number of reasons that this comment will discuss. Part II of this comment provides a background on the United States copyright law and the Government's efforts to combat infringement. Part III provides background on the Domain Name System and how seizure law relates to the domain name property. Part IV addresses the problems with the seizures by first discussing how the law which the Government claims the websites are violating, criminal copyright infringement pursuant to 18 U.S.C. § 506, is questionable because the domains are at most guilty of contributory copyright infringement, which is traditionally a civil claim. The Government must therefore ground its charges against the domains through aiding and abetting, which according to the seizure statute the Government is operating under, is not permitted. The second issue addresses due process concerns under the Fifth Amendment. Specifically, the seizures deprive the domain name owners of Constitutional protections by not permitting a pre-deprivation hearing. Lastly, many of the websites operating under the domain names may have

[1] U.S. INTELLECTUAL PROPERTY ENFORCEMENT COORDINATOR, 2010 U.S. INTELLECTUAL PROPERTY ENFORCEMENT COORDINATOR ANNUAL REPORT ON INTELLECTUAL PROPERTY ENFORCEMENT 14 (Feb. 2011), *available at* http://www.whitehouse.gov/sites/default/files/omb/IPEC/ipec_annual_report_feb2011.pdf [hereinafter IPEC 2010 ANNUAL REPORT].
[2] *Id.* at 14.
[3] *See* 18 U.S.C. § 2323(a)(1) (2008).

at least some protected speech and therefore by seizing the domains without previously determining that the domains are violating copyright law, is a prior restraint on speech and therefore violates the First Amendment.

A. PRESENT STATE OF DIGITAL PIRACY AND COSTS OF PIRACY

Piracy of copyrighted material such as music, movies and television broadcasts has been a major global issue for much of the past two decades. Ever since copyrighted works have become digitalized, there are more "opportunities for the appropriation of media products without compensation to their creators or producers."[4] Despite the efforts of companies such as Amazon.com, Apple, and Netflix to make digital media readily and legally available, many Internet users still choose to download pirated content from both illegal websites and Peer-to-Peer (P2P) networks.[5] The effect that this digital infringement has on the United States economy is significant. In 2005, it was estimated that losses due to piracy of copyrighted works were $25.6 billion and cost close to 400,000 American jobs.[6] Worldwide the losses have been estimated to be around $500-600 billion per year.[7]

According to a recent study, it is estimated that 23.76% of all global Internet bandwidth and 17.53% of United States Internet bandwidth is devoted to the storage and reproduction of infringing content.[8] Of that infringing content, only a small percentage is attributable to

---

[4] Robert G. Picard, *A Note on Economic Losses Due to Theft, Infringement, and Piracy of Protected Works*, J. MEDIA ECON., 207 (2004), http://oxford.academia.edu/RobertPicard/Papers/828359/A_note_on_economic_losses_due_to_theft_infringement_and_piracy_of_protected_works.

[5] Daniel Castro, *Better Enforcement of Online Copyright Would Help, Not Harm, Consumers*, INFORMATION TECHNOLOGY & INNOVATION FOUNDATION, 1 (Oct. 14, 2010), http://www.itif.org/files/2010-copyright-coica.pdf.

[6] Stephen E. Siwek, *The True Cost of Copyright Industry Piracy to the U.S. Economy*, INSTITUTE FOR POLICY INNOVATION, 1 (October 3, 2007), *available at* http://www.ipi.org/ipi%5CIPIPublications.nsf/PublicationLookupFullTextPDF/02DA0B4B44F2AE9286257369005ACB57/$File/CopyrightPiracy.pdf.

[7] *IPR Center Supports World Intellectual Property Day*, NEWS RELEASE, IPRCENTER.GOV (APR. 24, 2009), http://www.iprcenter.gov/partners/ice/news-releases/national-intellectual-property-rights-coordination-center-supports-this-sundays-world-intellectual-property-day.

[8] *Technical Report: An Estimate of Infringing Use of the Internet*, ENVISIONAL 55 (Jan. 2011), *available at* http://documents.envisional.com/docs/Envisional-Internet_Usage-Jan2011.pdf.

streaming traffic; however streaming services is the fastest growing area of the Internet and is believed to account for more than one quarter of all Internet activity.[9] Streaming sites such as YouTube do not seem to pose much of a threat, as much of the content posted is not copyrighted.[10] But even if a user manages to post copyrighted work, YouTube is very efficient in identifying this content and removing it expediently.[11] Sites such as LetMeWatchThis and Movie2k operate by providing numerous links to the latest movies and television shows that are available illegally for instant streaming through Flash-based video players.[12] These two sites represent only a few of many similar websites that provide links and streams to live televised sporting events and shows.[13] The artists and creators of the content on or linked to from these websites are ultimately harmed by this activity, and pass on the losses to the consumer in the form of increased prices and products of lesser quality.[14]

B. ROGUE WEBSITES

The websites discussed in the previous section have been named "rogue websites," and exist for the sole purpose of profiting from the distribution of things such as pirated movies and

[9] *Id* at 19.
[10] *Id*.
[11] *Id*. "YouTube itself prevents most users from uploading content longer than fifteen minutes in length and has added tools such as digital fingerprinting to ensure that copyrighted material is identified and banned…." *Id*. Not surprisingly, many times it is the owner of the work that seeks to have the work taken down, sometimes even . *See, e.g.*, Lenz v. Universal Music Corp., 572 F.Supp.2d 1150 (N.D. Cal. 2008) (A YouTube user posted a video of her young daughter singing and dancing to roughly 30 seconds of a copyrighted song. Universal sent YouTube a takedown notice pursuant to Title II of the Digital Millennium Copyright Act. The user sued claiming that Universal should knew or should have known that it was a self-evident non-infringing fair use).
[12] ENVISIONAL, *supra* note 8, at 20.
[13] Kat Asharyu, *Feds Crack Down on Illegal Live Sports Streaming*, ITVEDIA.COM (Feb. 3, 2011, 11:26 AM), http://www.itvedia.com/news/1300.html. (Government authorities seized ten websites for illegally streaming live sporting events, including National Football League games and pay-per-view events by World Wrestling Entertainment), *see* Sec. II *infra* (discussion about "rogue websites").
[14] Castro, *supra* at note 5, at 2. *See also Intellectual Property Theft: A Threat To U.S. Workers, Industries, And Our Economy*, DEPARTMENT OF PROFESSIONAL EMPLOYEES (Aug. 2010), *available at* http://dpeaflcio.org/pdf/DPE-fs_2010_intellectual_prop.pdf. (The loss in revenue from the theft and piracy of copyrighted films, television shows, theatrical productions, and music costs the U.S. entertainment industries billions of dollars in revenue each year, which ultimately effects the bottom-line profits and those who earn their living in these industries).

counterfeit drugs.[15] While these sites tend to take on a multitude of forms, one common denominator among them is that they all "materially contribute, facilitate and/or induce the illegal distribution of both stolen lawful products, such as movies and television programs, as well unlawful ones, such as counterfeit goods, including prescription medications."[16] Copyright enforcement efforts are often thwarted because the websites commonly appear to be legitimate content delivery sites, confusing both naïve consumers and those actively seeking evidence of infringement.[17] Not only are infringing websites difficult to identify, but they are also becoming increasingly more difficult to locate, as many are located outside the United States.[18] When the domain names are registered with a U.S. registry or registrar, the domain names are comparatively easier to seize.[19] Despite current efforts to combat these websites within the jurisdictional reach of the United States Government, there has also been recently proposed legislation that would allow the U.S. Government to effectively shut down access to foreign domain names.[20] This legislation, which has evolved into bills known as Stop Online Piracy Act (SOPA) and Preventing Real Online Threats to Economic Creativity and Theft of Intellectual Property Act (PROTECT IP Act or PIPA), have been extremely controversial.[21] As of early

[15] Richard Bennet, *Protecting Americans from Web scams*, NEW YORK POST (Dec. 29, 2011, 3:58 AM), http://www.nypost.com/p/news/opinion/opedcolumnists/protecting_americans_from_web_scams_lvOOEKJEqzpjGIAW43mIXP.
[16] *Id*.
[17] *The Growing Threat of Rogue Websites*, MOTION PICTURE ASSOCIATION OF AMERICA, *available at* http://www.mpaa.org//Resources/4aa9036c-ea05-4ada-8bee-6dc61b21335d.pdf (last visited Mar. 11, 2012).
[18] Maria A Pallante, Acting Register of Copyrights before the Subcommittee on Intellectual Property, Competition, and the Internet, Promoting Investment and Protecting Commerce Online: Legitimate Sites v. Parasites, Part I (Mar. 14, 2011), *available at* http://www.copyright.gov/docs/regstat031411.html; *see also* IPEC 2010 ANNUAL REPORT, *supra* note 1, at 14 (enforcement is complicated because of the limit of the U.S. Government's jurisdiction and resources in foreign countries).
[19] See *infra* Part III; Steven Seidenberg, *COICA Cracks Down on rogue Websites*, INSIDE COUNSEL (Jan. 2011), *available at* http://www.insidecounsel.com/2011/02/01/coica-cracks-down-on-rogue-websites.
[20] *The PROTECT IP Act: What You Need To Know*, CREATIVEAMERICA, http://www.creativeamerica.org/media/docs/ProtectIPAct.pdf (last visited Mar. 11, 2012).
[21] *Internet Blacklist Legislation*, ELECTRONIC FRONTIER FOUNDATION, https://www.eff.org/issues/coica-internet-censorship-and-copyright-bill (last visited Mar. 11, 2012).

2012, both bills remain stalled in Congress due to significant public opposition and outcry.[22] Several opponents warn that these two bills are unconstitutional and could quite possibly weaken or damage the Internet as a whole.[23] The constitutional issues implicated in both SOPA and PIPA are very similar to those issues addressed in this comment because in both instances, questions of due process and free speech invariably arise when Internet users and website owners are unilaterally prevented from accessing or distributing content on the web.

II. U.S. GOVERNMENT'S POWER TO COMBAT INFRINGMENT

The Constitution of the United States is the primary source of intellectual property protection in this country.[24] Clause 8 empowers Congress to grant, for a limited time, the exclusive rights to writings and discoveries of authors and inventors, respectively.[25] Congress has since statutorily delineated, through the Copyright Act of 1976, what works are entitled to copyright protection.[26] Whereas establishing copyright protection in this country has been relatively easy, enforcing copyrights has fallen significantly behind the technological age.[27]

A. DIGITAL MILLENIUM COPYRIGHT ACT

The first effort to bring copyright law up to date with the advent of digital copyrighted material came in the late 1990's. In 1998, Congress enacted, and President Bill Clinton signed

---

[22] David Goldman, *Millions in SOPA lobbying bucks gone to waste*, CNNMONEY (Jan. 27, 2012), http://money.cnn.com/2012/01/27/technology/sopa_pipa_lobby/?iid=Lead&hpt=hp_c1. Several major companies such as Google and Wikipedia staged a temporary boycott of their services in response to the bills. *See* Jaron Lanier, *The False Ideals of the Web*, NYTIMES.COM: THE OPINION PAGES (Jan. 18, 2012), http://www.nytimes.com/2012/01/19/opinion/sopa-boycotts-and-the-false-ideals-of-the-web.html.

[23] *See* Letter from Laurence Tribe, Professor, Harvard Law School to the Congress of the United States, *The "Stop Online Piracy Act" (SOPA) Violates The First Amendment* (Dec. 8, 2011); STEVE CROCKER, ET AL., SECURITY AND OTHER TECHNICAL CONCERNS RAISED BY THE DNS FILTERING REQUIREMENTS IN THE PROTECT IP BILL 2 (2011); Mark Lemley, et al., *Don't' Break the Internet*, 64 STAN. L. REV. ONLINE 34 (2011), *available at* http://www.stanfordlawreview.org/online/dont-break-internet.

[24] U.S. CONST. ART. I, §8, cl. 8.

[25] *Id*.

[26] *See* 17 U.S.C. § 102 ("…[O]riginal works of authorship fixed in any tangible medium of expression, now known or later developed, from which they can be perceived, reproduced, or otherwise communicated, either directly or with the aid of a machine or device.").

[27] Catherine Pignataro, *Copyright Law and the Internet: The New Generation of Legal Battles in the Courts*, 18 TOURO. L. REV. 783 (2002).

into law, the Digital Millennium Copyright Act (DMCA) of 1998, an amendment to Title 17 of the U.S. Code.[28] The DMCA was essentially a Congressional attempt to implement two World Intellectual Property Organization (WIPO) treaties: the WIPO Copyright Treaty and the WIPO Performances and Phonograms Treaty.[29] Once enacted, however, the DMCA actually provided more protection for copyright holders of digital material than the WIPO treaties had originally offered.[30]

Within the DMCA are two key provisions that specifically address the issue of copyright infringement with regards to digital content and protect content providers. First, an anti-circumvention provision disallows technological measures to bypass a work's own protections.[31] Second, the law prohibits any trafficking in any technology, product, service, device, component, or part thereof that would facilitate in the circumvention of copyright protections.[32] These two prohibitions in Chapter 12 effectively prohibit unauthorized access to copyrighted work as well as implement measures that prohibit copying of copyrighted work.[33]

An important exception to liability under the DMCA is the so-called "safe-harbor" provision that protects Internet service providers from the "intermediate and temporary storage" of infringing material on the network. The categories of exemption include transitory digital network communications, system caching, information residing on systems or networks at directions of users, and information location tools.[34] Assuming that the service provider lacked "actual knowledge" and also lacked "aware[ness] of facts and circumstances from which

[28] Pub . L. No. 105-304, 112 Stat. 2860 (Oct. 28, 1998).
[29] Digital Millennium Copyright Act of 1998, U.S. Copyright Office Summary, Dec. 1998, *at* 4-5.
[30] Jeffrey Cobia, Note, *Digital Millennium Copyright Act Takedown Notice Procedure: Misuses, Abuses, and Shortcomings of the Process*, 10 MINN. J.L. SCI. & TECH. 387, 388 (2009).
[31] 17 U.S.C. §1201(a) (2006).
[32] § 1201(b).
[33] Digital Millennium Copyright Act of 1998: U.S. Copyright Office Summary, Dec. 1998, *at* 4-5; *See also* JESSICA LITMAN, DIGITAL COPYRIGHT 143, (Pbk. Ed ed., Prometheus Books 2006).
[34] 17 U.S.C. § 512 (a)-(d) (2006).

infringing activity is apparent[,]" liability will not be imposed.[35] If, however, the provider has knowledge or awareness of infringement, it is the provider's responsibility to thereafter "act[] expeditiously to remove, or disable access to, the material…."[36] Most commonly this knowledge or awareness comes in the form of a takedown notice sent by the copyright holder to the service provider. Notice requirements are set out in section 512 and have several advantages to the service provider.[37] First, "[t]he DMCA notification procedures place the burden of policing copyright infringement—identifying the potentially infringing material and adequately documenting infringement—squarely on the owners of the copyright."[38] Secondly, the notification procedures also "provide the service provider with adequate information to find and examine the allegedly infringing material expeditiously."[39]

The DMCA has undoubtedly provided a powerful tool that copyright holders may use against online infringement; however, there have been strong criticisms that the notification procedures and takedown notices have a chilling effect on free-speech,[40] favor copyright holders with a large number of copyrights, and often show a "shoot now, ask later" mentality in regard to whether the potential infringement constituted fair use.[41]

B. PRO-IP ACT OF 2008

[35] § 512(c)(1)(A)(i).
[36] § 512(c)(1)(C).
[37] § 512(c)(3).
[38] Perfect 10, Inc. v. CCVill, LLC, 488 F.3d 1102, 1113 (9th Cir. 2007).
[39] House Report No. 551(II), 105th Congress, 2nd Session 1998, H.R. at 55.
[40] *See* Wendy Seltzer, Article, *Free Speech Unmoored in Copyright's Safe Harbor: Chilling Effects of the DMCA on the First Amendment*, 24 HARV. J. LAW & TECH. 171 (2010) (The takedowns resulting from DMCA notifications bear many of the hallmarks of prior restraints on speech).
[41] *See generally* Jeffrey Cobia, Note, *Digital Millennium Copyright Act Takedown Notice Procedure: Misues, Abuses, and Shortcomings of the Process*, 10 MINN. J.L. SCI. & TECH. 387(2009) (DMCA takedown procedure fails to enforce copyrights adequately, leads to violations of copyrights, and is used to censor criticism).

In October 2008, Congress passed the Prioritizing and Organization for Intellectual Property Act of 2008 (PRO-IP Act).[42] Overall, the PRO-IP Act made several changes to existing intellectual property law and provided the rights owners and federal law enforcement officials with new methods that could effectively enforce intellectual property rights.[43] At the time that PRO-IP was enacted, there had been a number of U.S. governmental agencies involved in protecting intellectual property rights.[44] These agencies included the Departments of Commerce, State, Justice, Health and Human Services, and Homeland Security; the U.S. Trade Representative; the U.S. Copyright Office; and the U.S. International Trade Commission.[45] From a purely administrative standpoint, PRO-IP helped coordinate interagency efforts by establishing the position of Intellectual Property Enforcement Coordinator (IPEC), whose responsibility was to develop a strategic plan with the agencies involved.[46]

The PRO-IP Act also increased criminal penalties and available civil remedies for counterfeiting and infringement,[47] but more importantly provided for the forfeiture[48] of any articles that were "used, or intended to be used, to commit or facilitate" the commission of various intellectual property offenses.[49] Forfeiture law was expanded significantly under this

---

[42] Prioritizing Resources and Organization for Intellectual Property (PRO-IP) Act of 2008, Pub. L. No. 110-403, 122 Stat. 4256 (2008) (codified as amended in scattered sections of 15-18, 42 U.S.C.).
[43] Alison Arden Besunder, *Righting the Wrong: Recovering Remedies for Trademark Infringement and Counterfeiting*, IP LITIGATOR, Sep.-Oct. 2009, at 1, *available at* http://www.besunderlaw.com/pdf/SeptOct2010-IP-Litigator-Righting-the-Wrong-Trademark-Infringement.pdf.
[44] U.S. GOV'T ACCOUNTABILITY OFFICE, GAO-11-39, INTELLECTUAL PROPERTY: AGENCIES PROGRESS IN IMPLEMENTING RECENT LEGISLATION, BUT ENHANCEMENTS COULD IMPROVE FUTURE PLANS 3 (2010).
[45] *Id*.
[46] *Id*. at 1, 5.
[47] Stephen J. Zraleck & Dylan Ruga, *The PRO-IP Act: Another Weapon Against a Failing Economy*, LANDSLIDE, Vol. 1, No. 3., at 34 (Jan/Feb 2009).
[48] Forfeiture is the divestiture of specific property without compensation, usually resulting from some default rule or legal action. Ensor v. Director of Revenue, 998 S.W.2d 782, 782, n.1 (Mo. 1999).
[49] 18 U.S.C. § 2323(a)(1)(A) (2008) (offenses include criminal copyright infringement, trafficking in counterfeit goods or labels falsely identifying copyrighted works as genuine, and unauthorized recordings of live music performances or films being shown in theaters). Property that may be seized pursuant to § 2323(a)(1)(A)-(C) include "[a]ny article, the making or trafficking of which is, prohibited under section 506 of title 17, or section 2318, 2319, 2319A, 2319B, or 2320, or chapter 90, of this title;" "[a]ny property used, or intended to be used, in any manner or part to commit or facilitate the commission of an offense referred to in subparagraph (A)," and "[a]ny property

change; under the old law, authorities could only seize criminally-infringing copies and any means by which infringing copies of the material could be reproduced.[50] ICE and the DHS use this statute as a powerful tool in seizing domain names that they believe to be involved in copyright infringement.[51]

C. ICE & OPERATION "IN OUR SITES"

The principal agency utilizing the Pro-IP Act to seize domain names has been the Immigration and Customs Enforcement agency. The ICE Office is the principal and largest investigative agency of the Department of Homeland Security and the second largest law enforcement organization in the United States, topped only by the FBI.[52] ICE has battled intellectual property theft since its inception in March 2003.[53] The U.S. Government has made the Internet its primary focus in the ongoing effort against the distribution of copyrighted material and counterfeit goods.[54]

In June 2010, ICE launched an initiative called Operation In Our Sites, aimed at preventing Internet counterfeiting and piracy by seizing domain names of websites providing access to infringing products.[55] In its first set of seizures, ICE executed seizure warrants against domain names of websites that were offering access to movies, many of which had just been

---

constituting or derived from any proceeds obtained directly or indirectly as a result of the commission of an offense referred to in subparagraph (A)." § 2323(a)(1)(A)-(C).

[50] 17 U.S.C. § 509(a) (repealed 2008).

[51] Terry Hart, *htmlComics: Domain Name Forfeiture Before Operation in Our Sites*, COPYHYPE (Sep. 7, 2011) http://www.copyhype.com/2011/09/htmlcomics-domain-name-forfeiture-before-operation-in-our-sites/.

[52] About ICE, *ICE Overview*, ICE.GOV, http://www.ice.gov/about/overview (last visited Mar. 11, 2012).

[53] Press Release, U.S. Dep't of Immigration & Customs Enforcement, ICE plays starring role in battling movie piracy: Operation In Our Sites, another successful intellectual property rights enforcement action (Jul. 2, 2010), http://www.ice.gov/news/releases/1007/100702hollywood.htm.

[54] IPEC 2010 ANNUAL REPORT, *supra* note 1, at 5.

[55] IPEC 2010 ANNUAL REPORT, *supra* note 1, at 4. Operation In Our Sites was only one part of the more expansive Joint Strategic Plan directed by the IPEC to ensure strong enforcement of American intellectual property rights. *Id*. at 1.

released in theaters.[56] One of the more notable seizures—the seizure of ChannelSurfing.net—occurred just prior to the Super Bowl and resulted in the arrest of the site's operator, Bryan McCarthy.[57] The site was dedicated to streaming both television programs and sports programs and reportedly made roughly $90,000 in advertising revenue prior to the seizure.[58] By early 2011, ICE had commenced five operations seizing 125 websites.[59]

The websites that were targeted come in three "flavors:" "linking," "cyberlocker," and "Bit torrent."[60] The linking websites often collect links to other websites that host infringing material and catalogue them so they are organized and easily accessible.[61] A link on a linking site can begin a download for the content or stream from a third-party server. Very rarely do these domains actually *host* the copyrighted material.[62] In contrast, cyberlockers are online storage servers that host a wide variety of digital media available for download through high-capacity data connections.[63] Bit torrent websites work differently than both cyberlockers and peer-to-peer programs such as Kazaa or Limewire. Bit torrents work by allowing multiple users—sometimes hundreds or even thousands—to download pieces of larger files such as

---

[56] *"Operation In OE, Manhattan U.S. Attorney seize multiple Web sites for criminal copyright violations*, News Releases, ICE.GOV (Jun. 30, 2010) http://www.ice.gov/news/releases/1006/100630losangeles.htm. The investigation resulted in the seizure warrants for seven domain names: TVSHACK.NET, MOVIES-LINKS.TV, FILESPUMP.COM, NOW-MOVIES.COM, PLANETMOVIEZ.COM, THEPIRATECITY.ORG, and ZML.COM. In an undercover capacity, investigators downloaded various newly released movies from the Web sites and their affiliates, to identify those Web sites that were involved in the distribution of stolen content. *Id*.

[57] David Makarewicz, *Arrest of Website Operator Renews Debate Over Constitutionality of Government Domain Seizures*, Mar. 9, 2011, http://www.sitesandblogs.com/2011/03/arrest-of-website-operator-renews.html.

[58] *Id*.

[59] 2011 U.S. INTELLECTUAL PROPERTY ENFORCEMENT COORDINATOR JOINT STRATEGIC PLAN: ONE YEAR ANNIVERSARY (Jun. 2011), *available at* http://www.whitehouse.gov/sites/default/files/omb/IPEC/ipec_anniversary_report.pdf [hereinafter IPEC ANNIVERSARY REPORT]

[60] Application and Affidavit For Seizure Warrant ¶ 12, In re 5 Domain Names, No. 10-2822M (C.D. Cal. filed Nov. 17, 2010) [hereinafter RapGodFathers.com Affidavit].

[61] *Id*.

[62] *See* Part IV.A. *infra* (discussing implications of contributory copyright infringement).

[63] RapGodFathers.com Affidavit, *supra* note 60, at ¶ 13.

movies or music.[64] Users with complete files "seed" to those users without the full file, who are called "leechers."[65] Leechers also share the pieces of files that they have with other leechers.[66]

III. THE PROPERTY: BACKGROUND ON THE DOMAIN NAME SYSTEM

The Internet is a decentralized, global network of interconnected computers,[67] where each computer is assigned an Internet Protocol address (IP address). An IP address is a series of four numbers ranging from 0-255, separated by periods.[68] These numbers allow computers to locate other computers on the Internet and exchange Internet traffic.[69] The Domain Name System (DNS) establishes a set of rules and procedures that help identify resources online, according to these IP addresses.[70] Those users who wish to host content on the Internet usually connect a computer to the Internet through a "server" which is then assigned an IP address by a particular Internet Service Provider (ISP).[71] It would be cumbersome and impractical for Internet users to remember each specific IP number associated with the desired content available on the Internet. Therefore, the DNS associates human-language with each respective IP address in the form of Uniform Resource Locators (URL's).[72] Human's can easily type in the URL that they wish to reach such as "www.YouTube.com" or "www.Amazon.com" and the DNS "resolves" this language into the respective computer-readable IP addresses.[73] Essentially what occurs is that

---

[64] Paul Gil, *Torrents 101: How Torrent Downloading Works*, ABOUT.COM (Nov. 2011), http://netforbeginners.about.com/od/peersharing/a/torrenthandbook.htm.
[65] *Id*.
[66] *Id*.
[67] *See*, Reno v. ACLU, 521 U.S. 844, 849-500 (1997) (describing the Internet as "an international network of interconnected computers).
[68] For example, Google's IP address is http://74.125.224.72. Typing this into an Internet browsers address bar will produce the same effect as inputting http://www.google.com/.
[69] RapGodFathers.com Affidavit, *supra* note 60, at ¶ 6.
[70] Kevin Werbach, *Castle in the Air: A Domain Name System for Spectrum*, 104 Nw. U L. Rev. 613, 622 (2010).
[71] MATTHEW MACDONALD, CREATING A WEB SITE 53 (2d ed. 2009).
[72] Orin Kerr, *The Problem of Perspective in Internet Law*, 91 GEO. L. J. 357, 363 (2003). For example "www.lawschool.com" would be an example of a URL that would have a corresponding IP address.
[73] Barry M. Leiner, et al., *A Brief History of the Internet*, INTERNET SOCIETY, http://www.isoc.org/internet/history/brief.shtml (last visited Oct. 11, 2011). "A domain name is a unique string of

the user inputs a unique name into their computer, which then queries the DNS server for the numerical IP address needed to connect to the content providing computers.[74]

The DNS is actually a hierarchy of names, organized in levels with the higher levels to the right.[75] For example in the domain "law.shu.edu", the Top-Level Domain (TLD) is ".edu", the second-level domain is "shu.edu", and the third-level domain is "law.shu.edu". Other top-level domains include ".com", ".net", ".org", ".mil" etc.[76] The Internet Corporation for Assigned Names and Numbers (ICANN) is responsible for coordinating all the technical elements of the DNS to ensure that all users are able to resolve to the desired content.[77] ICANN is responsible for delegating TLDs.[78] Under ICANN's system, a single company called a "registry" manages the domain names within a given TLD, and then contracts with different "registrars," who then offer the domain names to members of the public.[79] Individuals or businesses that buy the domain names are called "registrants."[80] Because registrants control the computer to which the IP address is assigned, a registrant may move a domain name to another computer anywhere in the world.[81]

Courts have historically disagreed on whether the domain names are considered property and thus available for seizure.[82] Congress made the issue clearer upon the enactment of the

---

characters or numbers that typically is used to designate and permit access to an Internet website." Mattel, Inc. v. Barbie-club.com, 310 F.3d 293, 295 (2d Cir. 2002).

[74] Ashley S. Pawlisz, *Legislative Update: The Bill of Unintended Consequences: The Combating Online Infringement and Counterfeit Act*, 21 DEPAUL J. ART TECH. & INTELL. PROP. L. 283, 286 (2011).

[75] Bill Stewart, *Internet Domain Names*, LIVING INTERNET, http://www.livinginternet.com/i/iw_dns_name.htm (last visited Oct. 13, 2011).

[76] *Id.*

[77] *About: ICANN*, ICANN (last modified Aug. 13, 2010), http://www.icann.org/tr/english.html (last visited Oct. 13, 2011).

[78] *Id.*

[79] *What Does ICANN Do?*, ICANN (last updated Aug. 13, 2010), http://www.icann.org/en/participate/what-icann-do.html.

[80] *Id.*

[81] *See* RapGodFathers.com Affidavit, *supra* note 60, at ¶ 6.

[82] *See* Kremen v. Cohen, 337 F.3d 1024 (9th Cir. 2003) (domain names satisfy the elements of the traditional test for property: they are capable of being precisely defined and exclusively controlled); *cf.* Network Solutions, Inc. v.

Anticybersquatting Consumer Protection Act (ACPA).[83] The ACPA permits trademark owners, in an action against a domain name connected with the protected trademark, to sue the domain name itself in an *in rem* proceeding.[84] The fact that the owner of the domain name could not be located for the proceedings is not an issue because "[s]ervice of process to the domain name registrar is deemed to constitute sufficient notice to the defendant.[85]

The procedure for seizing domain names is very straightforward.[86] The ICE agent, or appropriate governmental official, files with a court an application for warrant and an accompanying affidavit setting forth the grounds for seizure. If the application and affidavit show probable cause, a magistrate judge will issue the warrant. The warrant is then presented to both the domain name registry and the domain name registrar.[87] The registrar is then directed to lock the domain names pending the result of a forfeiture proceeding.[88] If the Government is awarded right and title to the subject domain names, the domain names are pointed to IP address 74.81.170.110, a Government IP address which has a notice stating, among other things, "This domain name has been seized by ICE – Homeland Security Investigations."[89]

This note will refer to both "seizures" and "forfeitures," but the terms are not interchangeable and are two distinct events even though, in practice, the two concepts can be

---

Umbro Int'l, Inc., 529 S.E.2d 80 (Va. 2000) (domain name is more analogous to a service contract and therefore could not be subject to garnishment)

[83] 15 U.S.C. § 1125(d) (2006).

[84] *Id*.; *See* Jack Mellyn, Note, *"Reach Out and Touch Someone": The Growing Use of Domain Name Seizure as a Vehicle for the Extraterritorial Enforcement of U.S. Law*, 42 GEO. J. INT'L L. 1241, 1249 (2011). "Under the *in rem* provision, the plaintiff may sue the domain name itself, with seizure or transfer of the domain as allowable remedies, and with the location of the domain name defined as the place where the *registrar*, not the defendant, is located." *Id*.

[85] Mellyn, *supra* note 84, at 1249.

[86] *See, e.g.*, RapGodFathers.com Affidavit, *supra* note 60, at Attachment A.

[87] *Id*.

[88] *Id*.

[89] *Id*.

very closely associated.[90] Seizure is the initial taking of the property in order to establish jurisdiction for a civil *in rem* proceeding,[91] or more commonly for the collection of evidence of crime for *in personam* proceedings.[92] This should be compared with forfeiture, which refers to the taking of property without giving compensation for it.[93] It is important to note that even though the seizure of property may be found illegal, this does not necessarily mean that the property cannot thereafter be forfeited.[94]

IV. PROBLEMS WITH THE SEIZURES

Many opponents to these seizures believe that the Government's claims against the domain names rest on somewhat questionable theories of law.[95] More specifically, the linking websites have been seized under the allegation of criminal copyright infringement; however, it is not likely that the sites themselves are guilty of direct copyright infringement due to the way the material is being provided. Furthermore, it has been highlighted that the ICE seizures and forfeiture proceedings may violate constitutional protections.[96] Both seizure and forfeiture have

[90] Marine Midland Bank, 11 F.3d 1119, 1124 (2d Cir. 1993) (citing United States v. Daccarett, 6 F.3d 37, 46 (2d Cir. 1993)); Terry Hart, *Feds Seize Domain Names*, COPYHYPE (Dec. 6, 2010) http://www.copyhype.com/2010/12/feds-seize-domain-names.

[91] The Brig Ann, 13 US 289, 291 (1815), "In order to institute and perfect proceedings *in rem*, it is necessary that the thing should be actually or constructively within the reach of the Court. It is actually within its possession when it is submitted to the process of the Court; it is constructively so, when, by a seizure, it is held to ascertain and enforce a right or forfeiture which can alone be decided by a judicial decree *in rem*;" *see also*, U.S. v. Jacobsen, 466 U.S. 109, 113 (1984) (seizure occurs when there is some meaningful interference with an individual's possessory interests in that property).

[92] 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, 745 (2009). Property is seized as evidence for *in personam* proceedings and used to determine the legal liability of the defendant. *Id*. It has never been doubted that search warrants could be issued for the seizure of contraband and the fruits and instrumentalities of crime. United States v. Lefkowitz, 285 U.S. 452, 465-66 (1932).

[93] *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, 745 (2009) (forfeiture is the actual divestitute of legal title in property by operation of law)

[94] U.S. v. Daccarett, 6 F.3d 37, 46 (1993).

[95] Mark Masnick, *Did Homeland Security Make Up A Non-Existent Criminal Contributory Infringement Rule In Seizing Domain Names?*, TECHDIRT (Jan. 6, 2011), http://www.techdirt.com/articles/20110104/12324012513/did-homeland-security-make-up-non-existent-criminal-contributory-infringement-rule-seizing-domain-names.shtml.

[96] *See*, *e.g.*, David Makarewicz, *5 Reasons Why the US Domain Seizures Are Unconstitutional*, Mar. 12, 2011, http://torrentfreak.com/5-reasons-why-the-us-domain-seizures-are-unconstitutional-110312/; David Makarrewicz,

procedural safeguards to limit the Government's power to seize an individual's property and ultimately forfeit that individual's interest in the property. Under the Fourth Amendment, seizures must be "reasonable" and must also be predicated on a warrant issued "upon probable cause."[97] The Supreme Court has held that while "[t]he Fourth Amendment does place restrictions on seizures conducted for purposes of civil forfeiture…it does not follow that the Fourth Amendment is the sole constitutional provision in question when the Government seizes property subject to forfeiture."[98] The seizures made possible under the Fourth Amendment must be accorded due process under the Fifth Amendment.[99] The Fifth Amendment Due Process Clause guards against the deprivation of an individual's life, liberty, and property without due process of law,[100] thus protecting deprivation without some sort of notice[101] and an opportunity to be heard.[102]

The seizure of domain names as property, as it turns out, is more than seizing an asset such as a yacht,[103] automobile[104], or even welfare benefits.[105] This is because while the domain name is property that may be seized,[106] the domain name may contain non-infringing, protected

---

Supporters of DHS Domain Name Seizures Undervalue Important Constitutional Protections, Mar. 28, 2011, http://www.infowars.com/supporters-of-dhs-domain-name-seizures-undervalue-important-constitutional-protections.

[97] U.S. Const. amend. IV.

[98] U.S v. James Daniel Good Real Property, 510 U.S. 43, 49 (1993); *See also* One 1958 Plymouth Sedan v. Pennsylvania, 380 U.S. 693, 696, 700 (holding that the exclusionary rule under the Fourth Amendment applies to civil forfeiture proceedings).

[99] *Id*. at 67. "Compliance with the standards and procedures prescribed by the Fourth Amendment constitutes all the "process" that is "due" to respondent…under the Fifth Amendment in the forfeiture context." *Id.* The Court in *James Daniel* cited to its decision in Gerstein v. Pugh, 420 U.S. 103 (1975), where it was discussed how the Fourth Amendment was "tailored explicitly for the criminal justice system" and the process due for seizures of person or property in criminal cases is the result of a "balance between individual and public interests." Gerstein v. Pugh, 420 U.S. 103, 125 (1975).

[100] U.S. CONST. amend. V.

[101] *See*, *e.g.*, Mullhane v. Central Hanover Bank & Trust Co., 339 U.S. 306 (1950) (discussing notice as a requirement of due process).

[102] *See*, *e.g.*, Goldberg v. Kelly, 397 U.S. 254 (1970) (hearing required before termination of welfare benefits).

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

[104] Krimstock v. Kelly, 306 F.3d 40 (2d Cir. 2002).

[105] *See Goldberg*, 397 U.S. 254.

[106] *See* Sec. II.B (discussing how a domain name is seizable property).

speech—such as chat rooms, discussion forums, and blog posts—that is afforded additional protection under the First Amendment.[107] These issues will be discussed in turn.

A. CRIMINAL COPYRIGHT INFRINGEMENT

To effectuate a seizure, ICE federal agents initially obtain a warrant by submitting a sworn affidavit to a Federal Magistrate Judge stating that in his or her opinion, and based on his or her expert training, it is believed that the websites within the domain in question are infringing copyright law.[108] The affidavits state there is "probable cause to believe that the [subject domain names] are property used, or intended to be used to commit or facilitate criminal copyright infringement in violation of 18 U.S.C. § 2319 [punishment guidelines] and 17 U.S.C. § 506 (a) [criminal copyright infringement], and are subject to seizure and forfeiture pursuant to 18 U.S.C. §2323(a)."[109] There is contention that these affidavits may have several factual and legal errors.[110] The most glaring legal error is that the affidavits allege that the websites' activity of embedding and linking to infringing content is a form of direct criminal copyright infringement.[111] The consensus among most courts is that mere linking to infringing content is not a form of *direct* copyright infringement.[112] To prove direct copyright infringement, the

---

[107] Andy Sellars, *The In Rem Forfeiture of Copyright-Infringing Domain Names*, May. 2011, available at http://papers.ssrn.com/sol3/papers.cfm?abstract_id=1835604&http://papers.ssrn.com/sol3/papers.cfm?abstract_id=1835604.

[108] *See, e.g.*, 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 Rojadirecta Affidavit].

[109] *Id*. at 4.

[110] Mike Masnick, *Full Homeland Security Affidavit To Seize Domains 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; Mike Masnick, *Full Affidavit On Latest Seizures Again Suggests Homeland Security Is Twisting The Law*, TECHDIRT (Feb. 3, 2011), http://www.techdirt.com/articles/20110203/01402812935/full-affidavit-latest-seizures-again-suggests-homeland-security-is-twisting-law.shtml; Mike Masnick, *Yes, The Legal & Technical Errors In Homeland Security's Domain Seizure Affidavit Do Matter*, TECHDIRT (Jan 4, 2011), http://www.techdirt.com/articles/20101229/01381312444/yes-legal-technical-errors-homeland-securitys-domain-seizure-affidavit-do-matter.shtml.

[111] Mike Masnick, *Full Affidavit On Latest Seizures Again Suggests Homeland Security Is Twisting The Law*, TECHDIRT (Feb. 3, 2011), http://www.techdirt.com/articles/20110203/01402812935/full-affidavit-latest-seizures-again-suggests-homeland-security-is-twisting-law.shtml.

[112] *See, e.g.*, Ticketmaster Corp. v. Tickets.Com Inc., 2000 WL 525390 (C.D.Cal.) ("[H]yperlinking does not itself involve a [direct] violation of the Copyright Act (whatever it may do for other claims) since no copying is

Government must initially show that the defendant has willfully infringed a copyright (1) for commercial or financial gain; (2) reproducing or distributing copies with a total retail value over $1000; or (3) making an unpublished work publicly available on a computer.[113] The difference between civil and criminal copyright infringement is that in addition to Government's burden of proving a valid copyright and infringement (the elements necessary for civil copyright infringement), the Government must also show willfulness and one of the qualifying violations of section 506(a)(1)(A)-(C).[114]

In cases when it is not possible to show that a defendant is liable for direct copyright infringement, liability may alternatively be established through indirect or secondary infringement on a theory of contributory or vicarious liability.[115] Contributory and vicarious liability are actually two subsets of secondary liability that have "emerged from common law principles and are well established in the law."[116] For a defendant to be found vicariously liable, the defendant must have both the right and the ability to control the individual that directly infringes, which thereafter results in a financial benefit for the defendant.[117] While this vicarious liability focuses primarily on the relationship between the defendant and the direct infringer, contributory liability focuses on the actions of the defendant and the intent or state of mind of the

involved."); Arista Records, Inc. v. MP3Board, 2002 WL 1997918, at *4 (S.D.N.Y. Aug. 29, 2002) (linking to content does not implicate distribution right and thus, does not give rise to liability for direct copyright infringement); Online Policy Group v. Diebold, Inc., 337 F.Supp.2d 1195, 1202 n.12 (N.D. Cal. 2004) ("Hyperlinking per se does not constitute direct copyright infringement because there is no copying").

[113] 17 U.S.C. § 506 (2008).

[114] *See* Daniel Newman, et al., *Intellectual Property Crimes*, 44 AM. CRIM. L. REV. 693, 717 (2007).

[115] *See* Metro-Goldwyn-Mayer Studios Inc. v. Grokster, Ltd., 545 U.S. 913 (2005) (*Grokster II*).

[116] Mark Bartholomew, *Cops, Robbers, and Search Engines: The Questionable Role of Criminal Law in Contributory Infringement Doctrine*, 2009 BYU L. REV. 783, 787 (2009).

[117] Perfect 10, Inc. v. Amazon.com, Inc., 487 F.3d 701, 729-30 (9th Cir. 2007).

defendant with regard to the direct infringement.[118] Contributory liability can be further separated into knowing facilitation and inducement.[119]

Inducement requires that the defendant encourage the direct infringer with the specific intent that the infringer will in fact infringe, often a difficult thing to prove.[120] Liability under a theory of knowing facilitation, however, requires that it be shown that the defendant have actual or constructive knowledge that their actions are likely to facilitate infringement by another and their actions must also materially contribute to the infringement.[121] Actual knowledge is not a requirement, and a court may infer knowledge of copyright infringement based on circumstantial evidence.[122] Courts are not entirely clear on what can constitute material contribution.[123] There is, indeed, scarce case law discussing whether linking to copyrighted conduct is a form of contributory copyright infringement, though the general trend has been in favor of the rights-holders.[124] The Ninth Circuit decision in *Perfect 10, Inc. v. Amazon.com, Inc.*, an adult website, Perfect 10, initiated suit against Amazon.com and Google, Inc. for the alleged infringement of pictures of its models.[125] In discussing the issue of material contribution in Perfect 10's claim against Google, the Court concluded that Google *did* materially contribute to the infringement by

---

[118] Sanford H. Kadish, *Complicity, Cause and Blame: A Study in the Interpretation of Doctrine*, 73 CAL. L. REV. 323, 337 (1985).
[119] PharmaStem Therapeutics, Inc. v. ViaCell, Inc., 491 F.3d 1342, 1358 (Fed. Cir. 2007); *See also* Gershwin Publ'g Corp. v. Columbia Artists Mgmt., Inc., 443 F.2d 1159, 1162 (2d Cir. 1971) ("[O] who, with knowledge of the infringing activity, induces, causes, or materially contributes
[120] Charles W. Adams, *Indirect Infringement from a Tort Law Perspective*, 42 U. RICH. L. REV. 635, 636 (2007).
[121] Bartholomew, *supra* note 116, at 788.
[122] *See* A&M Records, Inc. v. Napster, Inc., 239 F.3d 1004 (9th Cir. 2001) (the court inferred knowledge of copyright infringement based on Napster executives' illegal downloading activity, experience with copyrighted works, and knowledge of the recording industry).
[123] *See*, *e.g.*, *Napster*, 239 F.3d 1022 (9th Cir. 2001) (Napster materially contributes to infringement by providing a service in the form of a program that enables users to locate and download MP3 music files).
[124] *See*, *e.g.* Intellectual Reserve, Inc. v. Utah Lighthouse Ministry, Inc., 75 F.Supp.2d 1290 (D. Utah 1999) (preliminary injunction preventing a website from linking to copyrighted copies of books under contributory copyright infringement); Universal City Studios, Inc. v. Reimerdes, 111 F.Supp.2d 294 (S.D.N.Y. 2000) (court held that hackers contributorily infringed when they linked to software that descrambled DVDs so as to run on a Linux PC).
[125] 487 F.3d 701 (9th Cir. 2007).

"substantially assist[ing] websites to distribute their infringing copies to a worldwide market and assist[ing] a worldwide audience of users to access infringing materials."[126]

Whether the seized domains or the owners thereof would be civilly liable under contributory copyright infringement is debatable because the courts have not been consistent on these issues—such as what is sufficient to show material contribution, what mental state will support an inducement claim, or what contributions to infringement satisfy the requirements for inducement liability.[127] Certainly, according to Ninth Circuit precedent, it would be fair to say that the websites would be liable under contributory copyright infringement because of the actual or constructive knowledge that many of the sites link to almost exclusive copyrighted material, and that by compiling these links in a convenient location for Internet users, material contribution could also be established.

In the criminal context, conviction for copyright infringement based on secondary liability when another individual infringes is based on accomplice liability or aiding and abetting.[128] It has been argued that there are substantial problems with attempting to implement this type of *criminal* contributory liability through accomplice liability.[129] First, there is no indication that the Government seized any of the websites based on aiding and abetting.[130] Furthermore, the seizure statute, 18 U.S.C. § 2323, only allows for the seizure of property based

---

[126] *Id*. at 729.
[127] *See*, Bartholomew, *supra* note 116, at 790-92, 795.
[128] *See*, *e.g.* Venegas-Hernandez v. ACEMLA, 424 F.3d 50, 57-58 (1st Cir. 2005) (secondary copyright infringement is "a kind of abettor liability"); Sims v. W. Steel Co., 551 F.2d 811, 817 (10th Cir.
[129] *See generally*, Bartholomew, *supra* note 116 (Application of the rules of criminal accomplice liability to intellectual property disputes would dramatically alter the way contributory infringement claims are currently decided); Mark Masnick, *Did Homeland Security Make Up A Non-Existent Criminal Contributory Infringement Rule In Seizing Domain Names?*, TECHDIRT (Jan. 6, 2011), http://www.techdirt.com/articles/20110104/12324012513/did-homeland-security-make-up-non-existent-criminal-contributory-infringement-rule-seizing-domain-names.shtml.
[130] *See*, *e.g.*, Rojadirecta.com Affidavit, *supra* note 108.

on specific criminal statutes, of which aiding and abetting is not one.[131] Substantively, the Government will most likely run into problems in its pursuit of an aiding and abetting-type charge because it of course must be premised on at least one individual's criminal copyright infringement. This can be problematic depending on what type of website is linked. In the instances where the link is to a torrent file, it is unlikely that the Government will be able to show that each sharer of seeded torrents would be guilty of criminal infringement because it is extremely difficult to show the element of "commercial or financial gain" necessary for criminal infringement.[132] It may be somewhat easier to show infringement for sites that actually host the content and rely on user memberships and advertisement revenue, but problems arises when the sites are located outside the United States or, as in the cases of cyberlockers, when much of the content is managed by third parties. Ultimately, however, the biggest flaw rests on the lack of aiding and abetting as a ground for forfeiture. The Government, would have a stronger position to file charges against the website owners first rather than to improperly seize websites without the express authority to do so pursuant to Section 2323.

B. FIFTH AMENDMENT

Fundamentally, due process requires the opportunity to be heard at a meaningful time and in a meaningful manner.[133] It is very important that an opportunity to be heard is provided prior to the deprivation of property.[134] When property is seized, the general rules for civil forfeiture proceedings provide that notice be sent to the owners of the property once the property is seized

[131] 18 U.S.C. § 2323 (2006). Aiding and abetting can be found in 18 U.S.C. § 2 and 18 U.S.C. § 371.
[132] 18 U.S.C. § 506 (2006).
[133] Armstrong v. Manzo, 380 U.S. 545, 552 (1965).
[134] Fuentes v. Shevin, 407 U.S. 67, 81 (1983).

and before the commencement of a civil forfeiture action.[135] As discussed earlier, the owner of the domain names would be the party to be notified. After the seizure, the owner of the seized property "must file a claim with the appropriate official" to identify the property and establish their interest in the property.[136] Once this interested party has filed such a claim, the government has no later than ninety days with which to file a complaint for forfeiture.[137] If a complaint is filed, the interested party then has twenty days to file an answer to the complaint.[138] These procedures, provided by statute, seem to provide notice and a meaningful hearing that would therefore satisfy the Fifth Amendment, however, it is a different scenario when someone is accorded this process *after* they have been deprived of the property.[139]

Some form of a hearing is usually required before an individual is deprived of a property interest.[140] Having a party go through a petition process after the property has been taken defeats the purpose of the notice and hearing requirements. It follows that a hearing before a website owner is deprived of his or her property interest in a domain name is no different. In fact, the concept of due process is relatively flexible in that its procedural protections can be tailored to the demands of a particular situation.[141] To determine what appropriate form of hearing, if any, would comport with due process, the severity of the deprivation must be weighed.[142] But, while

---

[135] 18 U.S.C. § 983(a)(1)(A)(i)-(ii). "If the right to notice and a hearing is to serve its full purpose, then, it is clear that it must be granted at a time when the deprivation can still be prevented." Fuentes v. Shevin, 407 U.S. 67, 81 (1983).
[136] 18 U.S.C. § 983(a)(2)(A), (C) (2006).
[137] § 983(a)(3)(A).
[138] § 983(a)(4)(A)-(B).
[139] *See*, Mathews v. Eldridge, 424 U.S. 319, 332 (1976)(citing Wolff v. McDonell, 418 U.S. 539, 557-558 (1974)) ("This Court consistently has held that some form of hearing is required before an individual if finally deprived of a property interest"). There are some situations, especially in cases where the seized property is being used as evidence for a criminal trial, that there may be a pre-trial evidentiary hearing that would also satisfy the due process requirements. *See, e.g.*, United States v. One Learjet 24D, 191 F.3d 668,
[140] *Mathews*, 424 U.S. at 334. *See, also* U.S. v. E-Gold, Ltd., 521 F.3d 411, 417 (2008) (a pre-deprivation hearing is usually held in order to satisfy the notice and opportunity to be heard requirement of the due process clause of the fifth amendment).
[141] *Mathews*, 424 U.S. at 335 (discussing three factors that courts utilize to determine what process is due).
[142] U.S. v. Spilotro, 680 F.2d 612, 617 (E.D.Mich 1982).

helpful, this weighing is not always determinative of the right to a pre-deprivation hearing, and could imply that there are circumstances in which a pre-deprivation hearing is not available.[143] Indeed, in certain "extraordinary circumstances," pre-deprivation hearings may be dispensed with until after the seizure.[144] In *Fuentes v. Shevin*,[145] the Supreme Court held that a prejudgment replevin statute did not give procedural due process prior to a deprivation of property.[146] In its argument, the Court noted that in order to seize property without notice or hearing three specific criteria must be met to show that there are "extraordinary circumstances."[147]

1. The Seizures Satisfy An Important Governmental Or General Public Interest

In *Calero-Toledo v. Pearson Yacht Leasing Co.*,[148] the Supreme Court analyzed the seizure of a yacht under Puerto Rican law[149] where prior notice and a hearing were not given to the plaintiffs.[150] Analyzing the facts of the case using the three criteria necessary for "extraordinary circumstances," the Court first found that the seizure satisfied a significant governmental interest, specifically "assert[ing] *in rem* jurisdiction over the property in order to conduct forfeiture proceedings[.]"[151] This governmental interest "foster[s] the public interest in preventing illicit use of the property and in enforcing criminal sanctions."[152] The first of the *Fuentes* factors above requires the seizure be necessary to serve an important governmental

---

[143] *Id*.
[144] *Id*.
[145] 407 U.S. 67 (1972).
[146] *Id*. at 92-93.
[147] *Id*. at 91. "First, in each case, the seizure has been directly necessary to secure an important Governmental or general public interest. Second, there has been a special need for very prompt action. Third, the State has kept strict control over its monopoly of legitimate force: the person initiating the seizure has been a Government official responsible for determining, under the standards of a narrowly drawn statute, that it was necessary and justified in the particular instance." *Id*.
[148] 416 U.S. 663 (1974).
[149] P. R. Laws Ann., Tit. 24, §§ 2512 (a)(4), (b) (Supp. 1973).
[150] Calero-Toledo v. Pearson Yacht Leasing Co., 416 U.S. 663 (1974).
[151] *Id*. at 679.
[152] *Id*.

interest *or* public interest. The ICE seizures would certainly satisfy the governmental interest of seizing property for purposes of forfeiture under 18 U.S.C. § 2323; but, whether the public interest of protecting copyright laws and preventing these websites from operating would be sufficient to satisfy this element seems a debatable issue. Drug trafficking, as in *Calero-Toledo*, has much more of an effect on the "general public issue," whereas copyright and counterfeit violations affect only those rights-holders, and would at best have a tangential effect on the public as a whole. Regardless of whether the general public interest would be satisfied, the ICE seizures would most likely be a sufficient governmental interest to satisfy this first element.

2. There Is No Special Need For Very Prompt Action

The second element requires that "there…[be] a special need for very prompt action."[153] With regard to the yacht in *Calero-Toledo*, the Court reasoned that if there was pre-seizure notice and hearing, there would be a significant chance that the property "could be removed to another jurisdiction, destroyed, or concealed," thus frustrating the purpose of the statute.[154] This makes sense because, without the property, there could be no *in rem* jurisdiction. There have been situations in which any delay taken for notice and a hearing could lead to grave consequences. Such cases include instances when the public needed to be protected from contaminated food,[155] from a bank failure,[156] or from misbranded drugs.[157] It is true that studies have shown that copyright infringement and counterfeiting have serious financial effects on the United States, [158] but it is a stretch of the imagination to argue that it is of such importance that without the seizure of the websites, the public welfare would be at risk. Historically, some counterfeiters have used

[153] *Fuentes*, 407 U.S. at 91.
[154] *Calero-Toledo*, 416 U.S. at 679 (1974).
[155] North American Storage Co. v. Chicago, 211 U.S. 306 (1908).
[156] Coffin Bros. & Co. v. Bennett, 277 U.S. 29 (1928).
[157] Ewing v. Mytinger & Casselberry, Inc., 339 U.S. 594 (1950).
[158] *See* Section I.A (discussing the financial implication of copyright infringement).

websites to sell counterfeit drugs, resulting in death or injury.[159] If ICE had seized websites with probable cause that they were dealing in counterfeited drugs, prompt action would be much more appropriate.

For a purely evidentiary purpose, and not a jurisdictional one, an argument for the risk of destruction of the property is not persuasive. At the very least it would appear possible to document the content of the linking, cyberlocker, and Bit torrent websites for use as evidence, regardless of whether the owner of the domain shuts down the site after notice, or moves to another domain name. Under the General Rules for Civil Forfeiture, a claimant is entitled to the return of seized property under a certain set of proscribed circumstances.[160] In most of these circumstances, the Government will release property if there is little chance that the evidence will not be available for trial.[161] If, however, the claimant can show that the "likely hardship from the continued possession by the Government of the seized property *outweighs* the risk that the property will be destroyed, damaged, lost, concealed, or transferred if it is returned to the claimant during the pendency of the proceeding," the Government should immediately release the property.[162] The showing for hardship would be a case-by-case, fact-sensitive inquiry for each owner of the domains, though it would be possible that a claimant could make a showing that hardship combined with the fact that domains do not risk destruction prior to trial would entitle them to the return of their property.[163] Domain names usually remain under the control of

[159] *Counterfeit Internet Drugs Pose Significant Risks and Discourage Vital Health Checks*, SCIENCEDAILY (Jan. 20, 2010), http://www.sciencedaily.com/releases/2010/01/100120085348.htm.
[160] *See*, 18 U.S.C. § 983(f)(1) (2006).
[161] § 983(f)(1)(B)-(C).
[162] § 983(f)(1)(D).
[163] This is not the only situation in which the claimant may make a showing of hardship. It also may be shown that "the continued possession by the Government pending the final disposition of forfeiture proceedings will cause *substantial hardship* to the claimant, such as preventing the functioning of a business, preventing an individual from working, or leaving an individual homeless." 18 U.S.C. § 983(f)(1)(C).

the registry and registrars, thus could not be concealed or destroyed.[164] One domain owner has already filed a petition under 18 U.S.C. §983(f) to have the domain released due to "substantial hardship."[165]

3. The Federal Government Has Kept A Strict Monopoly Over The Copyright Enforcement

The final criterion under the *Fuentes* extraordinary circumstances test requires that "the State…kept strict control over its monopoly of legitimate force: the person initiating the seizure has been a Government official responsible for determining, under the standards of a narrowly drawn statute, that it was necessary and justified in the particular instance."[166] In *Calero-Toledo*, the Court held that the primary focus for this criterion is that the seizure was not implemented by self-interested parties and a Governmental official determines that the seizure is proper under a valid law.[167] This criterion would also be satisfied under the ICE seizures because a Government official (the ICE special agent) states in the affidavits that according to their "training and expertise," they feel both necessary and justified in the particular instance to seize the domain names pursuant to federal law.[168] It appears that the Court in *Calero-Toledo* gave deference to the Governmental officials, most likely under the presumption that a valid seizure warrant was issued based on enough evidence to show probable cause.[169]

In sum, the ICE seizures of domain names are unconstitutional under the Fifth Amendment because the website owners are not given due process—proper notice and a hearing—before they are deprived of their interest in the domain names. Even though there are

---

[164] Memorandum of Points and Authorities in Support of Puerto 80's Petition For Release of Seized Property and in Support of Request for Expedited Briefing and Hearing of Same 8, (S.D.N.Y. 2011) [Hereinafter Puerto 80 Petition].
[165] *See* Part C.
[166] *Fuentes*, 407 U.S. at 91; 18 U.S.C. § 983(f)(1)(C).
[167] *Calero-Toledo*, 416 U.S. at 679.
[168] *See*, RapGodFathers.com Affidavit, *supra* note 60. The statutes through which the ICE claims to act pursuant to are 18 U.S.C. § 2323 and 18 U.S.C. § 981.
[169] *Calero-Toledo*, 416 U.S. at 679.

circumstances where extraordinary circumstances justify a seizure without notice and a hearing, none exist here.

C. FIRST AMENDMENT

Of the domains seized by the DHS, only one owner has petitioned for the their domain's release.[170] Puerto 80 Projects, S.L.U. [hereinafter Puerto 80], is a Spain-based company that owns the rojadirecta.org and rojadirecta.com domain names, which are registered with GoDaddy.com, Inc.[171] Rojadirecta.com and rojadirecta.org were seized, along with eight other domains, shortly before Super Bowl XLV in the second set of ICE seizures of Operation In Our Sites.[172] Rojadirecta is a discussion group with various forums hosting topics such as sports and politics.[173] Within the sports forums, many users provide links to streams of sporting events and pay per view programs that are found elsewhere on the Internet.[174] Puerto 80 believed, and two Spanish courts agreed, that since the domains do not actually host the copyrighted videos or streams of sporting events, there was no infringement.[175] Following informal negotiations with the U.S. Attorney's Office, ICE and DHS, Puerto 80 filed an action for the return of the domains in the Southern District of New York.[176]

---

[170] Terry Hart, *Rojadirecta: Barking up the Wrong Tree?*, COPYHYPE (Aug. 9, 2011), http://www.copyhype.com/2011/08/rojadirecta-barking-up-the-wrong-tree/.
[171] Puerto 80 Petition, *supra* note 164 at 2.
[172] *See*, Rojadirecta Affidavit, *supra* note 108.
[173] Puerto 80 Petition, *supra* note 164 at 2.
[174] Puerto 80 Petition, *supra* note 164 at 3.
[175] Puerto 80 Petition, *supra* note 164 at 3. There are several factors that point to why, perhaps, Puerto 80 was the first company to file a petition against these seizures for return of the domain. First is the popularity of the site. As their petition recites, Rojadirecta has been listed among the 100 most popular sites in Spain in terms of traffic and boast approximately 865,000 registered users. Rojadirecta Affidavit, *supra* note 108 at 3. Secondly, they have the support of the Spanish courts, which they could perhaps argue for comity with regards to infringement. Lastly, of the sites seized by ICE, not all have forums for all visitors and members to discuss sports, politics, entertainment, etc.
[176] *Id*.; Terry Hart, *Rojadirecta Seeks Return of Seized Domain Names*, COPYHYPE (July 13, 2011), http://ww.copyhype.com/2011/07/rojadirecta-seeks-return-of-seized-domain-names.

Puerto 80 petitioned under 18 U.S.C. § 983(f)[177] for the release of the domains arguing that release was warranted pending the commencement and resolution of any forfeiture proceedings because "there [was] no risk that the domain names will be unavailable for any eventual trial, and Puerto 80 will continue to suffer substantial hardship—a reduction in traffic to Rojadirecta site and inability of…its users to access their accounts, in addition to a deprivation of First Amendment rights—if the domain names are not immediately returned…."[178] In essence, Puerto 80 argued that it suffered a substantial hardship for two reasons: the hindrance of the business of Puerto 80 and deprivation of First Amendment rights.[179] The Government responded to Puerto 80's petition by arguing that Puerto 80 failed to demonstrate substantial hardship under § 983(f)(1)(C) and, that, under the balancing test of § 983(f)(1)(D), the Government's interest would outweigh any hardship because Puerto 80 would be able to continue illegal activity on the websites.[180] The district court rejected Puerto 80's contention that the websites would lose business or customers because, at that time, Puerto 80 had "transferred its website to alternative domains which are beyond the jurisdiction of the Government."[181] The court noted that while the domains were out of reach of the Government's jurisdiction, U.S. residents could still access them without restriction.[182] The district court cursorily dismissed Puerto 80's argument that suppression of free speech is a *substantial hardship* within the meaning of § 983(f)(1)(C).[183] Relying on a similar reasoning with regard to Puerto 80's "loss of traffic argument," the district court recognized that the site's "main purpose" is to "catalogue links to the copyrighted athletic

[177] Puerto 80 Petition, *supra* note 164.
[178] *Id*. at 2.
[179] 18 U.S.C. § 283(f)(1)(C) states that a claimant is entitled to immediate release of seized property if…"the continued possession by the Government pending the final disposition of forfeiture proceedings will cause substantial hardship to the claimant, such as preventing the functioning of a business, preventing an individual from working, or leaving an individual homeless."
[180] Order, Puerto 80 Projects, S.L.U. v. U.S., 11 Civ. 3983 PAC 3 (Aug. 4, 2011) (S.D.N.Y.).
[181] *Id*. The new domain names included "www.rojadirecta.me," "www.rojadirecta.es," and "www.rojadirecta.in."
[182] *Id*.
[183] *Id*. at 4.

events" and the fact that visitors must go to other website to join in discussion is "not the kind of substantial hardship that Congress intended to ameliorate enacting § 983."[184] The judge noted that Puerto 80 could bring up its First Amendment argument in its upcoming motion to dismiss.[185]

Since the denial of the petition to have the domain name returned, but prior to filing a motion to dismiss in district court, Puerto 80 has filed for, and been granted, an expedited hearing by the Second Circuit.[186] In an opening brief, Puerto 80's stated the grounds for why it believes that the seizure of the Rojadirecta domains violates the First Amendment. Specifically, Puerto 80 argued that the district court's ruling to deny the return of the domains violates the First Amendment as a prior restraint by suppressing speech prior to making any determination as to the legality of that speech. The issue of whether these domain seizures are prior restraints is hardly black and white.[187]

Supreme Court jurisprudence holds that "prior restraints on speech and publication are the most serious and least tolerable infringement on First Amendment rights."[188] It is for this reason that systems that impose a prior restraint on speech come to court "bearing a heavy presumption against its constitutional validity."[189] With copyrighted speech, speech determined

[184] *Id*; *See* 145 Cong. Rec. H4854-02 (daily ed. June 24, 1999) (statement of Rep. Hyde) ("Individuals lives and livelihoods should not be in peril during the course of a legal challenge to a seizure.").
[185] *Id*. Some have incorrectly assumed that this ruling implies that the District Court is ruling that the seizures do not violate the First Amendment. *See Domain Seizures Do Not Violate Free Speech, U.S. Court Rules*, TORRENTFREAK, (Aug. 5, 2011) This is incorrect. The district court ruling states that a First Amendment argument is inappropriate for the purposes of a § 983 petition to show "substantial hardship."
[186] Mike Masnick, *Puerto 80 Explains How Rojadorecta Domain Seizures Violated the First Amendment*, TECHDIRT (Sep. 20, 2011), http://www.techdirt.com/articles/20110920/01444916022/puerto-80-explains-how-rojadirecta-domain-seizures-violated-first-amendment.shtml.
[187] *See*, *generally*, David Makarewicz, *5 Reasons Why the US Domain Seizures Are Unconstitutional*, TORRENTFREAK (Mar. 12, 2011), http://torrentfreak.com/5-reasons-why-the-us-domain-seizures-are-unconstitutional-110312.
[188] Nebraska Press Assn. v. Stuart, 427 U.S. 539, 559 (1976).
[189] New York Times v. U.S., 403 U.S. 713, 714 (1971).

to infringe copyright obviously does not avoid liability through the First Amendment.[190] Conversely, speech that does not infringe a copyright is afforded full First Amendment protection and subject to strict court scrutiny.[191] The seizures are no exception to the procedural protection of a judicial determination, a protection interpreted by the courts to be inherent in the First Amendment.[192]

1. The Content On The Websites Contains Protected Speech

The threshold issue in these cases is whether these or similar websites in question contain protected speech. While the courts application of the First Amendment to new electronic media has tended to lag, the Supreme Court has stated that websites are afforded full First Amendment scrutiny.[193] Based on these well-established principles, websites such as Rojadirecta.com, adthe.com, and any other website that hosts content on the Internet are presumptively accorded protection. This is not to say that the expressive works on the websites are legal. The Government has an opportunity to rebut this presumption by showing that any expression on a given website is illegal, and therefore not entitled to this protection. A website that is primarily dedicated to reproducing copyrighted works without authorization is nonetheless a controversial basis to enforce constitutional protections, given the chance that the Government may have a strong case to show criminality. Regardless of how strong the Government's case may be, there is no sliding-scale that would justify depriving the owners of the domains the opportunity to have their day in court to dispute the allegations. Further, as the District Court in the Puerto 80 case noted, it is clear that many of the forums that Puerto 80 relies on to show examples of protective

[190] Eldred v. Ashcroft, 537 U.S. 186, 221 (2003); *See* also, Marke A Lemley & Eugene Volokh, *Freedom of Speech and Injunctions in Intellectual Property Cases*, 48 DUKE L.J. 147, 167 (1998).
[191] *Eldred*, 537 U.S. at 221.
[192] Freedman v. Maryland, 380 U.S. 51, 58 (1965). "[O]nly a judicial determination in an adversary proceeding ensures the necessary sensitivity to freedom of expression [and] only a procedure requiring a judicial determination suffices to impose a valid final restraint." *Id.*
[193] Reno v. ACLU, 521 U.S. 844, 870 (1997). ("[O]ur cases provide no basis for qualifying the level of First Amendment scrutiny that should be applied to this medium.")

speech are merely ancillary to the website's primary purpose of providing access to copyrighted content.[194] The fact that a website has *some* portion of its website dedicated to forums or discussion boards—clearly protected speech—does not, and should not provide a haven for illegal activity, but courts also cannot limit constitutional protections prior to a determination that the site is breaking the law.

2. Domain Owners Are Entitled To First Amendment Procedural Protections

At the time the domains were seized, there was no court determination that any of the speech was infringing.[195] In fact, Puerto 80's motion for summary judgment was granted, which forced the Government to amend and re-file their complaint.[196] By not deciding whether the speech on the Rojadirecta website was entitled to protection, the U.S. Government improperly imposed a prior restraint on speech that should be granted First Amendment procedural protections.[197]

The affidavits that ICE presents to magistrates to have domains seized are based on probable cause, yet "mere probable cause to believe a legal violation has transpired is not adequate to remove [expressive content] from circulation."[198] The seizure of the domain names, however, does not take the content located on the server completely out of circulation.[199] In

[194] Order, Puerto 80 Projects, S.L.U. v. U.S., 11 Civ. 3983 PAC 4 (Aug. 4, 2011) (S.D.N.Y.) ("The main purpose of the Rojadirecta websties…is to catalog links to the copyrighted athletic events—any argument to the contrary is clearly disingenuous.").
[195] *Sellars*, *supra* note 107 at 17.
[196] Mike Masnick, *Court Dismisses Puerto 80 Rojadirecta Case (For Now)…But Doesn't Give Back The Domain*, TECHDIRT (Dec. 8, 2011), http://www.techdirt.com/articles/20111208/01424117003/court-dismisses-puerto-80-rojadirecta-case-now-doesnt-give-back-domain.shtml.
[197] *See* Fort Wayne Books, Inc. v. Indiana, 489 U.S. 46 (1989).
[198] *Id*. at 66. (defendant bookstores had engaged in a pattern of racketeering activity by repeatedly violating Indiana's obscenity laws).
[199] Order, Puerto 80 Projects, S.L.U. v. U.S., 11 Civ. 3983 PAC 3 (Aug. 4, 2011) (S.D.N.Y.) (the sites forums and message boards were up and running on different domains immediately following the seizures.). There has even been "plug-ins" for certain web browsers that would automatically redirect an internet user to the underlying IP address of the subject domain names. *Firefox Add-on 'Undoes' U.S. Government Domain Seizures*, TORRENTFREAK (Apr. 14, 2011), http://torrentfreak.com/firefox-add-on-undoes-u-s-Government-domain-seizures-110414.

Virginia State Pharmacy v. Virginia Citizens Consumer Council,[200] however, the Supreme Court disagreed with the reasoning that free speech could be abridged simply because the speaker or listener could go somewhere else and do it.[201] Following this logic, the district court's reasoning that Puerto 80 could notify its visitors of the new website domain name flies in the face of what the Supreme Court has already declared to be violative of the First Amendment.[202]

More recently, the Eastern District of Pennsylvania struck down a Pennsylvania statute that permitted the state's Attorney General or a district attorney to seek a court order requiring an ISP to take down websites accessible through the ISP that, upon a showing of probable cause, contained child pornography.[203] The statute imposed an unconstitutional restraint on speech.[204] The District Court analyzed Supreme Court precedent and concluded that a court must "make a final determination that material is child pornography after an adversary hearing before the material is completely removed from circulation."[205]

It is likely that the Second Circuit will find Rojadirecta's arguments compelling and for good reason. Regardless of whether the sites seized in Operation In Our Sites are infringing or contributorily infringing copyrights, the simple fact is that there is protected speech within at least some part of the sites. The Government, therefore, needs to implement procedural safeguards specifically tailored to ensure that the freedom of speech is not wrongfully abridged when expressive works are seized.[206] If the domain name, as the Government claims, is

---

[200] 425 U.S. 748 (1974).
[201] *Id* at 757 n.15. ("We are aware of no general principle that freedom of speech may be abridged when the speaker's listeners could come by his message by some other means…").
[202] Order, Puerto 80 Projects, S.L.U. v. U.S., 11 Civ. 3983 PAC 4 (Aug. 4, 2011) (S.D.N.Y.).
[203] Center for Democracy & Technology v. Pappert, 337 F. Supp. 2d 606, 619 (E.D. Pa. 2004).
[204] *Id*.
[205] *Id*. at 657.
[206] *See*, *Fort Wayne*, 489 U.S. at 62-63. For a great discussion on the recommended remedies, *see Sellars*, *supra* note 107.

facilitating copyright infringement, the domain is seizable. [207] This determination, however, must be made in a prompt judicial hearing with adequate notice.

Puerto 80 incorrectly argues in its opening brief that it believes that the Government must first prove Puerto's liability under the copyright laws before it can impose an injunction or similar remedy to prevent them from operating the sites in the proscribed manner.[208] This is incorrect because for an *in rem* civil procedure, it is the property that is the guilty party, not the owner.[209] Notwithstanding the fact that the Government may, as it deems necessary, seize the property without a conviction or charge the owner of the property with a crime, these website seizures stand apart from the general proposition that "a proceed *in rem* stands independent of, and wholly unaffected by, any criminal proceeding."[210] Puerto 80 seems to argue that since it has not, or believe that it cannot be proven guilty of infringement, the domains should be returned to them. They focus on the wrong problem here because their guilt has no connection with the involvement of the websites themselves with the infringement. The First Amendment argument, however, is the appropriate way in which Puerto 80 will succeed in this action, because while the guilt of the property is separate from Puerto 80, the First Amendment should protect them from being deprived of their property which ultimately could set bad precedent for other website owners that operate within the boundaries of the law.

V. CONCLUSION

Based on these observations, it seems clear that by seizing these domain names, the United States Government has overstepped its limits in several respects. The Government has

[207] *See*, 18 U.S.C. § 506 (2006).
[208] Opening Brief of Petitioner Puerto 80 Projects, S.L.U., Puerto 80 Projects S.L.U. v. U.S., 11-3390-cv (Sep. 12, 2011).
[209] *See* United States v. Bajakajian, 524 U.S. 321, 330 and n. 5, Calero-Toledo v. Pearson Yacht Leasing Co., 416 U.S. 663, 680-682.
[210] The Palmyra, 25 U.S. 1, 15 (1827).

the responsibility to pursue those that improperly infringe upon the rights of others, however this should be done within the confines of Congressional established law and the Constitution. Copyright infringement in these instances, when necessary, must be prosecuted through aiding and abetting, which according to seizure law, is not permissible. Furthermore, seizing domain names prior to a pre-deprivation hearing is improper under the Due Process Clause of the Fifth Amendment. Those domain names also may contain protected speech, which require further protections under the First Amendment to avoid a prior restraint on speech. These arguments do not, and should not, create the impression that violating copyrights is acceptable behavior. It is, however, unacceptable that the Government could use its power so unyielding without proper safeguards to protect those individuals that may get caught in the dragnet.