IP WARS: SOPA, PIPA, AND THE FIGHT OVER ONLINE PIRACY

Mike Belleville[*]

I. INTRODUCTION

In January of 2011, users who logged on to a number of popular video streaming web sites were greeted not with the usual homepage, but with a message from the Department of Homeland Security (DHS) stating that the web site had been seized by Immigration and Customs Enforcement (ICE).[1] The message merely explained that the domain name was seized in accordance with a warrant and cited 18 U.S.C. § 2319, the criminal copyright infringement statute.[2] These domain seizures were part of a wide-reaching campaign by ICE entitled "Operation in Our Sites." The goal of Operation in Our Sites is to shut down "commercial web sites engaged in the illegal sale and distribution of counterfeit goods and copyrighted works."[3] To date, the Operation has seized at least eighty-two domain names,[4] and has produced one conviction for criminal copyright infringement.[5] A number of the seized domains are run by foreign companies and operate completely outside the United States, with the exception of using a U.S. registered domain name.[6]

After the Operation began, two pieces of legislation, the Preventing Real Online Threats to Economic Creativity and Theft of Intellectual Property Act of 2011 (PIPA) and the Stop Online Piracy Act (SOPA), were introduced in the

---

* J.D. (expected May 2013), Temple University James E. Beasley School of Law; B.A. in International Affairs, George Washington University. The Author would like to thank Professor Donald P. Harris for his guidance and feedback throughout the writing process. The Author would also like to thank the staff of the Temple International & Comparative Law Journal for their hard work and assistance.

1. Ben Sisaro, *U.S. Shuts Down Websites in Piracy Crackdown*, N.Y. TIMES (Nov. 26, 2011), http://www.nytimes.com/2010/11/27/technology/27torrent.html.

2. An image of this message can be found at http://torrent-finder.com.

3. *ICE seizes 82 website domains involved in selling counterfeit goods as part of Cyber Monday crackdown,* US IMMIGRATION AND CUSTOMS ENFORCEMENT (Nov. 29, 2010), http://www.ice.gov/news/releases/1011/101129washington.htm.

4. *Id.*

5. *Founder of Ninjavideo Pleads Guilty to Criminal Copyright Conspiracy,* US IMMIGRATION AND CUSTOMS ENFORCEMENT (Sept. 23, 2011), http://content.govdelivery.com/bulletins/gd/USDHSICE-13cb8d.

6. Rojadirecta.com, for example, is operated by a Spanish company, and was found to be operating legally by Spanish courts. Bianca Bosker, *Rojadirecta.org One of Several Sites SEIZED By U.S. Authorities*, HUFFINGTON POST (Feb. 2, 2011, 11:13 AM), http://www.huffingtonpost.com/2011/02/02/rojadirecta-org-seized_n_817458.html.

House and Senate.[7] Both acts primarily target foreign "rogue" web sites which host or provide links to alleged copyright-infringing content.[8] The acts seek to strengthen copyright holders' rights[9] and expand their tools[10] to bring actions against foreign web sites believed to be infringing on their content. More recently, New Zealand authorities raided the home of Kim Dotcom and arrested him along with three other founders of Megaupload.com, a popular file storage web site.[11] The founders are undergoing extradition proceedings to the United States to be charged with criminal copyright infringement.[12] Both these events and the accts indicate an increased push, spearheaded by the United States, to address online piracy, which has become a pervasive global issue.

These actions, along with PIPA and SOPA, have raised a number of legal questions and have drawn criticism from a number of organizations and politicians.[13] In addition to raising questions of due process and First Amendment rights, the acts raise a number of questions in the realm of international copyright regulation and enforcement. These events have also raised a number of questions regarding piracy and the Internet. Concerns of censorship and overregulation of the Internet, as well as debates over the impacts of piracy and the proposed solutions' effectiveness, are at the forefront of these debates.

This Comment will examine the legal issues raised by SOPA and PIPA, as well as the United States seizure of the foreign web sites' domain names, and the effects these actions and legislation will have on Internet piracy. Primarily, this Comment will examine three key aspects of the debate: (1) what current protections and tools U.S. copyright holders have to combat online piracy; (2) how the proposed legislation expands these tools and what ramifications these expansions have, both domestically and internationally; and (3) what potential alternative solutions exist to address online piracy.

Part II of this Comment looks at the history of copyright infringement via the Internet; the evolution of peer-to-peer (P2P) file sharing; copyright infringement under current law; and U.S. copyright holders' existing protections and tools. Part II will also examine international treaties concerning copyright infringement and the ability of copyright holders to enforce their rights internationally. Part III examines the proposed legislation, PIPA and SOPA, which seeks to expand copyright holders' rights; how said legislation would affect and change current law; and other effects and impacts of such legislation. Part IV analyzes the legislation's strengths and weaknesses, examines the real impact of piracy, and

7. Julianne Pepitone, *SOPA Explained: What it is and why it matters*, CNNMONEY (Sept. 30, 2012), http://money.cnn.com/2012/01/17/technology/sopa_explained/index.htm.

8. *Id.*

9. *Id.*

10. *Id*.

11. *Megaupload Founder's Homes Raided, $5 Million in Luxury Cars Seized*, MSNBC (Jan. 20, 2011), http://technolog.msnbc.msn.com/_news/2012/01/20/10199528-megaupload-founders-homes-raided-5m-in-luxury-cars-seized.

12. *Id.*

13. For a detailed discussion, see *infra* Section IV-C.

proposes alternative potential solutions to the issue of international online piracy.

II. THE RISE OF INTERNET PIRACY AND THE CURRENT LEGAL FRAMEWORK

A. The Rise of Internet Media and Digital Piracy

The Internet's rapid rise has created many challenges for copyright law. Along with the increased popularity of the Internet came the increased popularity of P2P, torrent, and other web sites and programs that created new ways for people around the world to share files.[14] People have an underlying desire to share—indeed, it is taught to every child at a young age—and as such, people embrace new means of sharing. The ability to share any file—a picture, a document, a song, or a movie—nearly instantly is an immensely appealing concept, and one that, at a fundamental level, does not feel inherently wrong. Of course, when millions of files are being exchanged, it is inevitable that copyrighted content will be shared, intentionally or not.[15] While many users who share content have no intention of sharing copyrighted content (and many are often unaware that what they are doing is illegal), there are, of course, others who do so purposefully. The anonymous nature of the Internet, the ease of access to content, and the relatively low (or seemingly low) chance of being caught provides those seeking to intentionally share copyrighted content with an appealing means of doing so. These factors all led to the rapid expansion of file sharing on the Internet.

When Napster, an early P2P program, emerged in 1999, millions of Internet users were suddenly able to download any file their fellow users were willing to share for free. Prior to Napster's introduction, file sharing on the Internet was limited in scope, primarily due to the fact that it generally required a greater understanding of the Internet and of computers than a user-friendly program like Napster.[16] Napster, like all P2P programs, was capable of sharing both legal (i.e., non-copyrighted) as well as illegal (i.e., copyrighted) files. Napster was a small program that a user could install on almost any computer. Once installed and connected to the Internet, the program allowed a user to search for a file they wished to download. The program would then search the files made available by other users who were also logged onto the program. If a match were found, then the user could download the file to his computer, making a copy of the original.

---

14. For an overview of some of the copyright challenges created by the Internet, see generally Fredrick Oduol Oduor, *The Internet and Copyright Protection: Are We Creating a Global Generation of Copyright Criminals?*, 18 VILL. SPORTS & ENT. L.J. 501 (2011).

15. *Id.*

16. Prior to the release of programs such as Napster, Internet users were able to share files using networks and programs such as Usenet, Internet Chat Relay, and FTP servers. These programs were significantly less popular than the types used today, and for the non-tech savvy, much more complex to use. Since the bulk of legal decisions relevant to this Comment came after their use, they will not be discussed in detail here. For a detailed discussion, see generally ANDY ORAM, PEER-TO-PEER: HARNESSING THE POWER OF DISRUPTIVE TECHNOLOGIES (2001), *available at* http://oreilly.com/catalog/peertopeer/chapter/ch01.html.

Napster itself provided no files, but simply provided a means of connecting users willing to share files.

Another class of P2P programs, called torrents, took a more arms-length approach to file sharing. Torrent programs required the user to download a program that could download "tracker" files.[17] Tracker files are small files that contain a list of users who have a particular file and are willing to upload it to another user.[18] These files are kept on torrent index web sites, such as the highly popular thePirateBay.se.[19] These index web sites do not host any actual content themselves, but only the tracker or lists of users who have the files.[20] The torrent programs themselves likewise do not contain any content, but merely connect users together.[21] As with earlier P2P programs, the torrent system can be used to share legal and illegal content. Torrents operate by a process called "data-swarming."[22] This process allows a person downloading a file to upload file portions to other users while continuing to download the remaining portion of the file.[23] This process allows for faster, more efficient downloads, as well as expanding the number of users involved in a single instance of file sharing.

As Internet speeds increased, so did the possibilities for sharing content. In 1995, a radio broadcast of a baseball game was streamed live across the Internet.[24] In 2005, YouTube emerged, allowing millions of users to upload, share, and view videos via the Internet.[25] The site quickly gained popularity and, almost as quickly, faced complex legal issues. YouTube could not stop users from uploading copyrighted content, and given the volume of videos uploaded, could not view and monitor all of them. It is therefore the responsibility of individual copyright holders to issue a takedown notice when they find infringing content.[26] YouTube

---

17. *See* Adam Pash, *A beginner's guide to BitTorrent*, LIFEHACKER (Aug. 3, 2007, 12:00 PM), http://lifehacker.com/285489/a-beginners-guide-to-bittorrent#b2 (stating that users must first download a "BitTorrent client" before they can begin downloading the files they seek). Popular programs of this nature include Bitorrent and Utorrent.

18. Kevin Bauer, Dirk Grunwald & Douglas Sicker, *The Challenges of Stopping Peer-to-Peer File Sharing* (Univ. of Colo. Dep't of Computer Science, 2009), *available at* http://www.mit.edu/~ke23793/papers/Kevin_NCTA_talk.pdf.

19. Thepiratebay.se was formerly located at thepiratebay.com and switched its domain name to the Swedish domain ".se" only recently in response to the domain seizures and legislation discussed in this Comment. The reasons the site would make such a switch are discussed *infra* text accompanying notes 102-107.

20. Paul Gil, *Torrents 101: How Torrent Downloading Works*, ABOUT.COM, http://netforbeginners.about.com/od/peersharing/a/torrenthandbook.htm (last visited Oct. 22, 2012).

21. *Id*.

22. Miaoran Li, *The Pirate Party and The Pirate Bay: How the Pirate Bay Influences Sweden and International Copyright Relations,* 21 PACE INT'L L. REV. 281, 286 (2009).

23. *Id.*

24. Daniel Akst, *The Cutting Edge: COMPUTING/ TECHNOLOGY/ INNOVATION: Take Me Out to the Internet? Tune in to Baseball on the Web*, L.A. TIMES (Sept. 6, 1995), http://articles.latimes.com/1995-09-06/business/fi-42764_1_internet-users.

25. Jim Hopkins, *Surprise! There's a third YouTube co-founder*, USA TODAY (Oct. 11, 2006), http://www.usatoday.com/tech/news/2006-10-11-youtube-karim_x.htm.

26. *See infra* text accompanying notes 34-59 (discussing notice and takedowns).

has faced numerous lawsuits from large entertainment companies.[27] The popularity of sites such as YouTube prompted a rise in "on-demand" or streaming video content. In 2007, popular movie rental by mail company Netflix introduced an online streaming option, allowing subscribers to instantly watch a movie via the Internet.[28] Other major companies including Apple, Comcast, and HBO have also introduced such services.[29] A majority of these services negotiate licensing agreements with copyright holders or are run by the rights holders themselves, and are therefore perfectly legal.[30]

Most recently, "cloud computing" technologies have provided a platform for users to share and store content.[31] Popular versions of such technology include Megaupload, RapidShare, Dropbox, and Apple's iCloud. These types of services provide users with storage space "in the cloud," which means users' data is stored on a server offsite and not (necessarily) on their hard drive. A user can upload files to the cloud and access these files from other computers and devices. Such services store a user's files on the service provider's own servers. This allows a user easy backup and access to files regardless of device or computer used. By actually storing files for a user, these companies can potentially be exposed to liability because a user can just as easily upload copyrighted content as legitimate content.

Given the popularity and ease of such technology, a vast number of web sites have emerged providing streaming content of copyrighted material, often without negotiating a license from the copyright holder.[32] These sites either provide live streams, pre-recorded videos, or links to streams and videos of TV shows, movies, and sports events.[33]

B. Current Legal Framework for Copyright Enforcement in the United States

As these technologies formed and became heavily utilized, the law began to change along with them. This Section provides an overview of the current legal

---

27. *See infra* text accompanying notes 84-91.

28. Michael Liedtke, *Netflix Expands Internet Viewing Options,* SAN FRANCISCO GATE (Jan. 13, 2008), http://web.archive.org/web/20080115195018/http://www.sfgate.com/cgi-bin/article.cgi?f=/n/a/2008/01/13/financial/f090113S93.DTL.

29. Wilson Rothman, *Xbox pre-emptively strikes at Apple iTV with Comcast, HBO, MLB*, NBC NEWS (Mar. 28, 2012), http://www.nbcnews.com/technology/ingame/xbox-pre-emptively-strikes-apple-itv-comcast-hbo-mlb-569049.

30. Atul Patel, *Defying the Gravity of Cable Giants: HBO Nordic AB and Its Implications,* IMEDIA CONNECTIONS (Oct. 3, 2012), http://blogs.imediaconnection.com/blog/2012/10/03/defying-the-gravity-of-cable-giants-hbo-nordic-ab-and-its-implications/.

31. Rivka Tadjer, *What is Cloud Computing?,* PCMAG.COM (Nov. 18, 2010), http://www.pcmag.com/article2/0,2817,2372163,00.asp.

32. *Two Top Administrators of NinjaVideo Website Plead Guilty to Criminal Copyright Conspiracy*, DEPARTMENT OF JUSTICE (Oct. 25, 2011), http://www.justice.gov/opa/pr/2011/October/11-crm-1403.html.

33. *Id.* These sites are often based in foreign countries for a variety of reasons, including the fact that copyright laws in some countries are more flexible and allow the sites to operate. Popular examples of such sites include tvlinks.com, ninjavideo.com, and rojadirecta.com.

framework as it relates to online piracy.

1. The Copyright Act

The Copyright Act of 1976 gives a copyright owner a number of rights including, *inter alia,* the right to reproduce in copies, distribute copies, perform publicly, and publicly display copyrighted works.[34] The copyright owner also has the ability to license these various rights.[35] The copyright owner additionally has the ability to control the work's distribution.[36] The exclusive right to public performance gives the copyright holder the ability to control the work's live performance, as well as the playing of the work's recording in a public area.[37] These are the rights typically involved in infringement cases involving the Internet. Movies, songs, video games, and the like are the most common copyrighted content exchanged using P2P services. Videos and songs are frequently found on YouTube and other streaming sites, as well as broadcasts and recordings of live events such as sporting events.

The Copyright Act, however, was most recently amended in 1976, long before online copyright infringement became an issue. Legislators in 1976 could not have contemplated or foreseen the Internet's impact on copyrights. Since the most recent amendment of the Copyright Act, Congress has passed two statutes attempting to address the realities of online infringement. The first, the Digital Performance Right in Sound Recordings Act of 1995 (DPRSRA), gave copyright holders the right to perform their works digitally.[38] The DPRSRA essentially allows copyright holders to require a license for others to stream audio works via the Internet.[39] The second relevant statute enacted since the 1976 Copyright Act, and the primary statute governing digital copyright infringement, is the Digital Millennium Copyright Act (DMCA) of 1998.[40]

2. The Digital Millennium Copyright Act (DMCA)

The DMCA attempts to provide a framework to address copyright infringement that occurs on the Internet. The DMCA serves a few primary functions. First, it implements the World Intellectual Property Organization (WIPO) Copyright and Performances and Phonograms Treaties Implementation Act, which greatly expands U.S. copyright law by including works produced in almost any WIPO member country.[41] The second provision, which is often called

---

34. Copyright Act of 1976, 17 U.S.C § 106 (1976).
35. *Id.* § 204(a).
36. *Id.* § 106(3).
37. *Id.* § 106(4–6).
38. *Id.* § 106(6).
39. *Id.*
40. Digital Millennium Copyright Act of 1998, Pub. L. No. 105-304, 112 Stat. 2860 (codified as amended in scattered sections of 17 U.S.C.) [hereinafter DMCA].
41. *Id.* § 102. For a full list of WIPO member countries, see *Member States,* WORLD INTELLECTUAL PROPERTY ORGANIZATION, http://www.wipo.int/members/en/ (last visited Oct. 22, 2011).

the DMCA anti-circumvention provision, serves to restrict the ability to make, sell, or distribute means to circumvent digital rights management systems.[42] The DMCA also heightens the penalties for online infringement.[43]

In an effort to reduce the potential liability faced by legitimate sites, the DMCA includes what are known as "safe harbor" provisions. These provisions shield online service providers (OSPs)[44] from liability for direct and secondary copyright infringement in certain situations.[45] To qualify for safe harbor protection, an OSP must have a policy in place that removes repeat offenders from the service.[46] In addition to this general requirement, the DMCA imposes additional requirements for each of the four safe harbors provided in the Act. For the purposes of this Comment, only the safe harbor provisions of § 512(c) are relevant and will be discussed.[47] Section 512(c) of the DMCA applies to OSPs that store infringing material online. It imposes three requirements for OSP immunity to liability: (1) the OSP must not receive any financial benefit directly attributed to the infringing conduct;[48] (2) the OSP must not have actual or circumstantial knowledge of the infringing content;[49] and (3) the OSP must, upon notice from the copyright holder, act to remove the infringing content.[50]

The DMCA does not impose an affirmative duty upon an OSP to police its services for infringing content.[51] Instead, an OSP can be put on notice either by the copyright holder or by the so-called "red flag" test.[52] This test examines whether the "infringing activity would be apparent to a reasonable person operating under the same or similar circumstances."[53] The ambiguity of this provision raises the most questions regarding the liability of many web sites.

The DMCA's safe harbor provisions, in general, lean towards protecting the

---

42. DMCA, *supra* note 40, § 103 (stating that digital rights management systems are technologies that limit or control an individual's use of a copyrighted work, and common examples include serial numbers for software programs or encryption and scrambling systems that prevent making copies of films).

43. *Id.* § 1204 (establishing that penalties can be as high as a $500,000 fine or up to five years imprisonment for a first offense, and a $1,000,000 fine or up to ten years imprisonment for subsequent offenses).

44. "Online service provider" includes Internet service providers such as Comcast as well as web sites such as Google. *See id.* § 512(k)(1) (providing the definition of "service provider").

45. *Id.* § 512 (showing that direct infringement occurs when a party personally violates a right of the copyright owner, and indirect infringement occurs when a third party enables or aids a party in infringing the rights of a copyright holder).

46. *Id.* § 512(i)(1)(a).

47. For more information on the three other safe harbor provisions, see *id.* §§ 512(a)–(b),(d).

48. DMCA, *supra* note 40, § 512(c)(1)(B).

49. *Id.* § 512(c)(1)(A).

50. *Id.* § 512(c)(1)(C).

51. *See* H.R. REP. NO. 105-551, pt. 2, at 53 (1998) (discussing the knowledge standard of § 512(c)).

52. *Id.*

53. *Id.*

OSPs from liability. In 2008, the Ninth Circuit held in *Perfect 10, Inc. v. CCBill, LLC*[54] that the burden of proof is not placed on the service provider to determine whether content is infringing or not.[55] In reaching this conclusion, the court noted that there is no way for a service provider to easily determine whether the material is infringing, and the court was not willing to impose "investigative duties" on service providers.[56] In 2009, the District Court for the Central District of California severely limited what could be considered a "red flag" for the purposes of putting a service provider on notice.[57] The court concluded that if certain facts and circumstances require investigation by the service provider to determine whether content infringes copyrights, then those facts and circumstances are not "red flags."[58] In 2010, a New York District Court concluded that "[g]eneral knowledge that infringement is 'ubiquitous' does not impose a duty on the service provider to monitor or search its service for infringements."[59] It is clear that the DMCA's safe harbor provisions typically have been construed in favor of the OSPs and have placed a majority of the burden on copyright holders to monitor their own copyrights.

3. Case law

In addition to statutory law, the United States has developed significant case law dealing with digital copyright infringement. Much of this case law involves the interpretation of terms within the DMCA. Napster's success prompted a highly publicized lawsuit. In 2000, the Recording Industry Association of America (RIAA) brought suit against Napster on behalf of a number of record companies.[60] The suit reached the Ninth Circuit, which affirmed the district court's holding that Napster, and presumably other P2P networks, could be held liable for contributory and vicarious copyright infringement of any copyrighted work illegally downloaded using its software.[61] The court found that a vast majority of the content available on Napster was copyrighted.[62] The court also held that Napster was contributorily liable for the infringement of its program users because Napster had knowledge of the infringing content and materially contributed to the infringement.[63] The court additionally found Napster vicariously liable because it received financial gain from the infringement and was in a position to monitor the use of its program.[64] This was the first major case to address the application of copyright laws to P2P file-sharing programs, and the decision opened up providers

54. 488 F.3d 1102 (9th Cir. 2007).
55. *Id.* at 1113.
56. *Id.* at 1114.
57. UMG Recordings, Inc. v. Veoh Networks, Inc., 665 F. Supp. 2d 1099 (C.D. Cal. 2009).
58. *Id.* at 1108.
59. Viacom Int'l, Inc. v. YouTube, Inc., 718 F. Supp. 2d 514, 525 (S.D.N.Y. 2010).
60. A&M Records v. Napster, 239 F.3d 1004 (9th Cir. 2001).
61. *Id.* at 1027.
62. *Id.* at 1013.
63. *Id.* at 1020–22.
64. *Id.* at 1023–24.

of such programs to significant liability under the doctrines of contributory and vicarious liability.

Following the decision in *A&M Records v. Napster*, a number of P2P programs faced similar lawsuits. In 2005, twenty-eight of the largest entertainment companies sued Grokster, a P2P file-sharing client similar to Napster.[65] Grokster operated slightly differently from Napster in that users interacted directly with one another and not through a central server. Grokster merely provided a gateway to a network that users accessed to share files.[66] Users then interacted directly with each other to share files. As a result, Grokster had reduced knowledge of its users' activities as they did not pass through a central server operated by Grokster. It, additionally, had no means to control these activities. Grokster, like many P2P programs, could be used for non-infringing purposes such as the transfer of public domain e-books, original works distributed by the authors themselves, and so on. However, the court found that 90% of the files exchanged using Grokster were copyrighted.[67] Additionally, one of Grokster's stated objectives was the use of the network for infringement.[68] In finding Grokster liable for infringement, the Supreme Court held that "one who distributes a device with the object of promoting its use to infringe copyright, as shown by clear expression or other affirmative steps taken to foster infringement, is liable for the resulting acts of infringement by third parties."[69] The Supreme Court further concluded that vicarious liability required a financial interest in the infringing conduct and a failure to stop the infringer.[70] Additionally, the defendant could be contributorily liable if it intentionally induces or encourages the infringement.[71] The *Grokster* decision solidified the potential liability a P2P software provider can face when allowing users to access infringing content. Significantly, *Grokster* solidified the potential for liability for indirect infringement even when there is a non-infringing use for a service or technology.[72]

The knowledge requirement of the DMCA § 512(c) safe harbor provisions was tested and interpreted in 2009 in *UMG Recording, Inc. v. Veoh Networks, Inc.*[73] Veoh Networks operates in a similar manner to YouTube; it hosts videos posted by both commercial and personal users. These videos can be streamed by users online or downloaded. Like most web sites that allow user uploaded content, Veoh inevitably hosted copyrighted content. In holding Veoh not liable under a § 512(c) defense, the court concluded that "actual knowledge" under the DMCA

65. Metro-Goldwyn-Mayer Studios Inc. v. Grokster, Ltd., 545 U.S. 913 (2005).
66. *Id.* at 921.
67. *Id.* at 922.
68. *Id.* at 923–24.
69. *Id* at 919.
70. *Id.* at 930.
71. *Metro-Goldwyn-Mayer Studios Inc.*, 545 U.S. at 930.
72. *Id.* at 934.
73. 665 F. Supp. 2d 1099 (C.D. Cal. 2009).

requires specific, actual knowledge of infringement by a specific posting.[74] The court further concluded that the burden rests with the copyright owner to provide the service provider with notice (and thus knowledge) of the actual infringing content, and that notice of certain instances of infringement does not provide knowledge for any other specific infringement on the site or infringement generally.[75]

The court in *Veoh* went on to conclude that the "red flag" provision of the DMCA, designed to prevent a site from purposefully avoiding knowledge of infringement, is a high bar; moreover, if the knowledge and facts a site needs to circumstantially conclude infringement require investigation on the part of the service provider, then the knowledge and facts are not a "red flag."[76] General knowledge that some content may be infringing is not enough to establish the requisite knowledge for liability.[77] Allowing such general knowledge to void a service provider's access to the safe harbor provision, the court stated, would defeat the purpose of such a provision.[78] *Veoh* solidified that the knowledge requirement of the DMCA goes beyond mere "general knowledge" that infringement can or has happened in small quantities on a site.[79]

The United States has had less success holding torrent web sites liable for copyright infringement than it has with Napster-like P2P services for a number of reasons. Torrent web sites merely provide links to infringing content and do not host any infringing content themselves.[80] This makes the sites similar to search engines such as Google and Bing, which typically fall within the DMCA safe harbor provisions.[81] The law is unclear and unsettled with regard to the legality of the linking to infringing content. There have been a few decisions by lower courts that have held web sites liable in certain circumstances. One such circumstance is when a site uses links to avoid a previously issued injunction against copyrighted content posted on their site.[82] Another circumstance is when the site provides links to devices or programs designed to circumvent copyright infringement.[83] It is still unclear how the law should treat these torrent sites. The links they provide are user-submitted, and at least some of the links provided do not direct users to copyrighted content.

U.S. law has addressed the issue of copyrighted content in regards to content sites, such as YouTube. In 2010, for example, Viacom brought suit against

---

74. UMG Recordings, Inc. v. Veoh Networks, Inc., 665 F. Supp. 2d 1099, 1108 (C.D. Cal. 2009).

75. *Id.* at 1110–11.

76. *Id.* at 1108.

77. *Id.* at 1111.

78. *Id.*

79. *Id.* at 1108–1112 (providing useful analysis of actual knowledge versus an awareness of facts and circumstances that falls beneath the knowledge threshold set forth in the DMCA).

80. Gil, *supra* note 20.

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

82. *See* Intellectual Reserve, Inc. v. Utah Lighthouse Ministry, Inc., 75 F. Supp. 2d 1290 (D. Utah 1999).

83. *See* Universal City Studios, Inc. v. Reimerdes, 111 F. Supp. 2d 294 (S.D.N.Y. 2004).

YouTube seeking $1 billion in damages for copyrighted content posted by users of the site.[84] Viacom alleged that "tens of thousands of videos on YouTube" violated its copyrights.[85] Viacom formulated its complaint based on a database of user-usage information that the court had previously ordered YouTube to give to Viacom.[86] The court held that YouTube was protected by the wide breadth of the DMCA safe harbor provisions and therefore could not be held liable for damages.[87] Specifically, the court concluded that the "[m]ere knowledge of prevalence of such activity in general is not enough" to show knowledge of infringement and thus precludes a safe harbor defense.[88] The court also took note of the differences in distribution models between YouTube and services like Grokster, noting that YouTube's existence as a legitimate service was far different from that of Grokster or Napster, which existed solely for the purpose of infringement.[89] Furthermore, YouTube had effective notice and takedown provisions in place,[90] as well as a policy of banning repeat offenders.[91] *Viacom* creates clear protections for services similar to YouTube, which seek to provide a legitimate service to consumers, but, due to their nature, simultaneously provide a method for copyright infringement. Interestingly, the decision appears to suggest that well-established web sites will be treated more favorably under the DMCA than newer sites.

In summary, current U.S. case law established a few principles for determining contributory and vicarious liability under the DMCA. First, a web site that maintains some form of a copyright compliance and enforcement program will be more likely to avoid liability than one that does not.[92] Second, the volume and percentage of infringing versus non-infringing conduct that occurs on a service or program is important.[93] Third, the knowledge required to void a safe harbor defense varies depending on a number of factors—including compliance programs and volume of infringement—but a more specific knowledge of infringement is required than a mere understanding that infringement generally occurs on a platform.[94] Finally, it is important to factor in any revenue or benefit an OSP may receive as a result of infringement.[95]

On the other hand, case law has not fully established what types of web sites

84. Viacom Int'l, Inc. v. YouTube, Inc., 718 F. Supp. 2d 514 (S.D.N.Y. 2010).

85. *Id.* at 518.

86. Viacom Int'l, Inc. v. YouTube, Inc., 253 F.R.D. 256 (S.D.N.Y. 2008).

87. *Viacom*, 718 F. Supp. 2d at 527.

88. *Id.* at 523.

89. *Id.* at 525–26.

90. *Id.* at 519.

91. *Id.* at 527–28.

92. Christian E. Mammen, *File Sharing is Dead! Long Live File Sharing! Recent Developments in the Law of Secondary Liability for Copyright Infringement,* 33 HASTINGS COMM. & ENT. L.J. 443, 458 (2011).

93. *Id.*

94. *Id.*

95. *See id.* (reasoning that since sites linking to infringing content attract more traffic, such sites can generate extra revenue from advertising on the sites).

and online services will face secondary and contributory liability from infringing conduct. Much gray area exists and many areas of the DMCA have yet to be interpreted. However, case law makes it clear that the inquiry must be done on a case-by-case basis. Each web site or platform must be evaluated on its own, with the factors discussed above driving the inquiry. As if this inquiry were not enough, the jurisdictional issue also arises, as the DMCA, of course, only applies to sites and services that fall under U.S. jurisdiction.

C. Extraterritorial Application of U.S. Copyright Law

One striking feature of the major U.S. cases on digital infringement is the absence of any international or extraterritorial issues. So far, courts have not dealt significantly with these types of web sites and programs that operate on an international level. These issues, however, are quickly becoming relevant. As current U.S. efforts such as Operation In Our Sites made clear, copyright infringement is increasingly occurring on foreign web sites. The inherently multinational nature of the Internet makes this a murky legal issue. This Section will explore the current state of the extraterritorial application of U.S. copyright law and how it interacts with the current state of digital infringement laws.

As a baseline, there is a strong presumption against the extraterritorial application of U.S. copyright law.[96] At its strictest, this means that unless an actual infringement occurs within the United States, U.S. courts lack jurisdiction.[97] This principle is derived from the idea that Congress has the constitutional ability to enact statutes reaching conduct outside the United States, but only when Congress "clearly manifests" intent for a specific statute to have extraterritorial application.[98] Therefore, the party seeking to apply a statute to conduct occurring outside the United States has the burden of affirmatively showing that the statute applies extraterritorially.[99] The Copyright Act contains no explicit language authorizing its extraterritorial application.[100] This presumption has been challenged a number of times in court, but the courts determined that Congress did not intend the Copyright Act to have extraterritorial application.[101]

This raises questions as to where online activity occurs and where sites are "located." A domain name is considered property.[102] This property is said to be

96. *See* Subafilms, Ltd. v. MGM-Pathe Commc'ns Co., 24 F.3d 1088, 1093–98 (9th Cir. 1994) (stating that it is an "undisputed axiom" that U.S. copyright laws do not apply extraterritorially).

97. 7 PATRY ON COPYRIGHTS § 25:86 (2011).

98. *Id.*

99. *Id.*

100. 17 U.S.C. § 501 (1976) (stating that anyone who violates an owner's rights is an infringer under the statute without expressly stating that this includes extraterritorial persons or entities).

101. 7 PATRY ON COPYRIGHTS § 25:86; *see generally* Omega S.A. v. Costco Wholesale Corp., 541 F.3d 982 (9th Cir. 2008) (discussing and weighing arguments in favor of and against applying the first sale doctrine of copyright to conduct outside the United States).

102. Kremen v. Cohen, 337 F.3d 1024, 1030 (9th Cir. 2003).

located where the domain names registry is located.[103] This idea was based on the provision of the Anticybersquatting Consumer Protection Act (ACPA), which primarily deals with trademark infringement.[104] Under the ACPA, courts have *in rem* jurisdiction over domain names in the places where they are registered.[105] Thus a domain name's physical location depends on its top level domain, which is a small tag following the actual domain name such as ".com" or ".net."[106] Any web sites with a ".com" or ".net" top level domain name are hosted at a registry operated by Verisign, Inc. in Virginia.[107] A district court in Virginia would therefore have *in rem* jurisdiction over these web sites.

This is significant because it allows the U.S. government to exercise *in rem* jurisdiction over a site that is otherwise entirely foreign, so long as they have a domain name located at a registry within the United States. In the case of a site such as rojadirecta.com, which has all of its servers located in Spain and is operated by a Spanish company, the domain name is subject to U.S. jurisdiction and, as was the actual case, can be seized under court order as other property can.

D. International Law

New technologies give rise to the need to address intellectual property issues and piracy on an international level. The Internet's spread makes this particularly true for copyright law. International copyright issues are handled primarily by the World Trade Organization (WTO) and the World Intellectual Property Organization (WIPO), and specifically through two treaties: The Berne Convention ("Berne") and Trade-Related Aspects of International Property Agreement ("TRIPS").

1. The Berne Convention

The Berne Convention was originally enacted in 1886.[108] The United States joined Berne in 1988. Since its enactment, Berne has undergone a number of revisions but its general purpose and character has remained the same. The primary purpose of Berne is to protect the rights of works' authors.[109] To ensure authors' rights are respected internationally, the convention establishes minimum standards to which all countries that are party to the agreement must adhere.[110] These

103. Office Depot Inc. v. Zuccarini, 596 F.3d 696, 702–03 (9th Cir. 2010).

104. *See generally* Anticybersquatting Consumer Protection Act (ACPA), 15 U.S.C. § 1125(d) (2009).

105. *Id.* § 1125(d)(2)(A).

106. See *infra* notes 168-176 and accompanying text for a more complete discussion of the domain name system.

107. *Domain Name Services*, VERISIGN, INC., http://www.verisigninc.com/en_US/products-and-services/domain-name-services/index.xhtml.

108. Peter Burger, *The Berne Convention: Its History and Its Key Role in the Future*, 3 J.L. & TECH. 1, 15 (1988).

109. *Id.* at 16.

110. *Id.*

minimums, of course, do not prevent a country from offering greater protections, but create a floor of protections which a country must provide. One of the primary standards under Berne is the concept of national treatment.[111] National treatment means that parties to Berne must give foreign authors the same rights they would give their own citizens.[112]

In addition to this key provision, Berne also lists a number of rights that authors must be given, such as the right to reproduction of the work, and contains a list of works covered by Berne. Berne, which was enacted over 100 years ago, has undergone significant revisions throughout the years. These revisions primarily extended the list of covered works to include new forms of media, and expanded certain rights authors have when dealing with new technologies (such as broadcasting).[113] Since its enactment, each revision has served to expand the rights of authors.[114] Today the convention covers any expression of literary and artistic works–essentially anything that is copyrightable.[115] Notably, since Berne does not provide any mechanism for international enforcement, member countries that do not comply do not face penalties.

2. Trade-related aspects of international property agreement

The enforcement issue is addressed by TRIPS. The TRIPS agreement was enacted through the WTO in 1994.[116] In addition to covering copyrights, TRIPS addresses nearly every area of intellectual property protection, including patents, trademarks, and trade secrets. TRIPS incorporates, as a starting point, the rights given to authors in the Berne Convention.[117] In addition, TRIPS expands on these rights and creates new, higher standards of protection.[118]

Most significantly, TRIPS creates an enforcement mechanism for WTO members. TRIPS requires that all signatories provide the enforcement mechanisms listed in the agreement. The agreement lists a number of enforcement requirements and includes provisions covering evidentiary and procedural rules, as well as provisions for both civil and criminal enforcement of copyrights.[119] The enforcement provisions have been summarized as requiring countries to meet six "performance standards" so that procedures: (1) permit effective action against infringement; (2) allow expeditious remedies to prevent infringement; (3) deter further infringement; (4) are not unreasonably compacted; (5) are not unreasonably costly; and (6) do not have time limits which cause unwarranted delays or that are

111. *Id.* at 12.

112. *Id.* at 17.

113. *Id.* at 33.

114. Burger, *supra* note 108, at 20–50 (highlighting each revision's expansion of rights).

115. *See id.* at 43 (discussing Stockholm revision's abolishment of fixation requirement).

116. *Intellectual Property: Protection and Enforcement,* THE WORLD TRADE ORGANIZATION, http://www.wto.org/english/thewto_e/whatis_e/tif_e/agrm7_e.htm.

117. *Id.*

118. *Id.*

119. *Id.*

too short.[120] These standards are general and countries may bring enforcement actions against other countries for inadequate enforcement.

On their own, Berne and TRIPS do not provide a solution to the type of copyright infringement and piracy that occurs on the Internet today. The minimum standards created in both agreements do not reach the levels that many U.S. officials and copyright holders would like. The Berne Convention's lack of an enforcement mechanism makes it of little use to a country seeking a remedy to infringement other than providing some guiding principles of what protections a country should have.

The enforcement arm of TRIPS has problems of its own. The general and imprecise nature of the enforcement provisions are often criticized, with some commentators describing the provisions as the agreement's "Achilles heel."[121] By providing only broad legal standards, TRIPS' enforcement provisions make it difficult for disputes between countries to be settled, as the disputes will often boil down to disagreements over interpretations of provisions' general language definitions.[122] TRIPS' provisions do not apply to any countries not party to the treaty.

This issue is easily illustrated by the recent dispute between the United States and China over China's enforcement of intellectual property laws. China, a party to TRIPS, has been continuously accused by the United States of failing to live up to the enforcement standards of the agreement. Specifically, the United States felt that China's criminal enforcement provisions were weak, it failed to dispose of infringing goods, and it declined to provide protection to works banned by the Chinese government that would otherwise be protected.[123] The dispute highlighted the issues created by the vague and broad principles outlined in TRIPS and had a very real impact on the ability of countries to force their peers to meet certain levels of enforcement.

Current disputes highlight the ineffectiveness of TRIPS' enforcement provisions as well. In the case of Rojadirecta, discussed above, the United States believed that a web site which provides links to infringing content violates copyright law,[124] while the Spanish courts did not.[125] There is very little that the United States could accomplish using the TRIPS provisions because the provisions do not define what exactly constitutes infringement. Spain has a system for enforcement of copyrights in place, and if that system determines an action is not an infringement, then there is little that the United States can do under TRIPS.

---

120. INT'L INTELLECTUAL PROP. ALLIANCE, COPYRIGHT ENFORCEMENT UNDER THE TRIPS AGREEMENT 2 (2004), *available at* http://www.iipa.com/rbi/2004_Oct19_TRIPS.pdf.

121. Peter K. Yu, *TRIPS and Its Achilles' Heel,* 18 J. INTELL. PROP. L. 479, 482 (2011).

122. *Id.*

123. Peter K. Yu, *The Trips Enforcement Dispute,* 89 NEB. L. REV. 1046, 1053–54 (2011).

124. Memorandum of Points and Authorities in Support of Claimant's Motion to Dismiss at 8, U.S. v. Rojadirecta.org, 11 Civ. 4139 (S.D.N.Y. 2011).

125. *Id.* at 3.

III. PROPOSED LEGISLATION

Before proceeding to look at new legislation, it is important to take stock of the tools covered in the preceding sections that a U.S. copyright holder and the U.S. government currently have to combat piracy. Copyright holders have the ability to send notice and takedown requests to web sites under the DMCA. Copyright holders also have the ability under the DMCA to issue takedown notices to search providers such as google.com to remove links to infringing content from search results. The United States has the ability to exercise jurisdiction *in rem* over foreign web sites that have domain names on registries located in the United States. This gives the U.S. government the ability to bring criminal copyright claims against the web site and potentially take other actions, including seizing the domain. Finally, the U.S. government has the ability under TRIPS to bring a claim against another TRIPS member country for failing to meet the minimum protections established by the agreement. This gives the government an indirect means of fighting foreign copyright-infringing web sites by, in theory, forcing a country that has lax enforcement standards to increase them. The next Section will examine what new mechanisms pending legislation would provide to copyright holders.

Through a lobbying effort totaling over $91 million, the content industry, including the RIAA and MPAA, indicated to Congress that they were unsatisfied with the current state of copyright enforcement in the United States.[126] Operation In Our Sites is currently one of the primary tools that the United Sates is employing to combat online piracy and infringement. After the operation began, and presumably in response to lobbying efforts, two bills, PIPA and SOPA, were introduced in the House and Senate. Since the implementation of the Operation and the announcement of both bills, the legislative efforts have received significant coverage, both positive and negative, in the intellectual property community and the media. Throughout most of 2011, media coverage was scarce and the bills enjoyed significant support in Congress. Large web sites, including Wikipedia and Reddit, as well as technology companies began to speak out against the bills, with opposition efforts culminating in a blackout of thousands of sites, including Wikipedia on January 18, 2011, in protest of the bill.[127] Following the blackout both bills lost a number of congressional supporters, including co-sponsors of the bills.[128] This Section will first look at what is proposed in both PIPA and SOPA. It will then briefly examine the policy arguments both for and against the use of such techniques and PIPA and SOPA in general.

---

126. Jenifer Martinez, *Shootout at the Digital Corral,* POLITICO (Nov. 16, 2011), http://www.politico.com/news/stories/1111/68448.html.

127. Ned Potter, *Wikipedia Blackout: Websites Wikipedia, Reddit, Others Go Dark Wednesday to Protest SOPA, PIPA,* ABC NEWS (Jan. 17, 2012), http://abcnews.go.com/Technology/wikipedia-blackout-websites-wikipedia-reddit-dark-wednesday-protest/story?id=15373251#.T0rDM_VZBTE.

128. Grant Gross, *Internet's Protest Prods US Senate to Delay Vote,* PC WORLD (Jan. 20, 2012), http://www.pcworld.com/article/248466/internets_protest_prods_us_senate_to_delay_vote.html.

A. Preventing Real Online Threats to Economic Creativity and Theft of Intellectual Property Act of 2011 (PIPA)[129]

Introduced in May of 2011 by twelve senators from both parties, PIPA is one of two legislative measures that attempt to address the problems associated with online piracy. The bill itself is aimed directly at foreign web sites that, as discussed above, are difficult to bring under U.S. jurisdiction.[130] According to the Senate Committee on the Judiciary, the bill attempts to respond to the estimated billions of dollars copyright piracy costs U.S. creators and producers of copyrighted works every year.[131]

According to the drafters, the Act is aimed at "the most egregious rogue websites that are trafficking in infringing goods."[132] The text of the bill describes these web sites as those that have "no significant use" other than copyright infringement.[133] The Act would give the Attorney General, as well as certain "qualified plaintiffs," the ability to bring an action against entirely foreign web sites, provided a showing can be made that the web site has a connection to the United States.[134] Connection is broadly defined as any web site that "harms holders of United States intellectual property."[135] "Qualified plaintiffs" are defined as any intellectual property rights holders.[136] This greatly expands the rights of intellectual property rights holders as they will not need to wait for the government to bring a suit. A rights holder is able to get a temporary restraining order, preliminary injunction, or an injunction that cuts the web site off from consumers in the United States by filtering its domain name for search engines and redirecting its domain name.[137]

In addition, the Attorney General may order four classes of third parties to comply with measures to cut off the "rogue" web site from U.S. users.[138] These four classes are: (1) operators of domain name servers (DNS);[139] (2) financial transaction providers (such as Paypal); (3) Internet advertisers; and (4) "information location tools."[140] By allowing actions against these third parties,

---

129. S. 968, 112th Cong. (2011) [hereinafter PIPA].

130. Michelle Sherman, *PROTECT IP Act: One Approach To Dealing With Internet Piracy,* 15 J. INTERNET L. 3 (Oct. 2011).

131. S. REP. NO. 112-39, at 2 n.3 (2011).

132. *Id.* at 8.

133. PIPA, *supra* note 129, §§ 2(7)(A)(i)–(iii) (2011) (as passed by the Senate Judiciary Committee but placed on hold by Senator Ron Wyden in May 2011).

134. *Id.* § 3(a).

135. *Id.* § 3(b)(1)(B)(ii).

136. *Id.* § 2(11)(b).

137. *Id.* § 3(b)(1).

138. *See id.* § 3(a) (showing that other qualified plaintiffs may compel action only against financial transaction providers and Internet advertisers).

139. DNS providers provide web sites with a named address that users can enter to reach a web site (such as www.google.com). Without a named address, users would only be able to access a site by entering the IP address of the web site.

140. PIPA, *supra* note 129. Information location tool provider takes the same definition

PIPA would ensure that once an action is brought against a foreign web site, the United States can (1) filter its domain name and remove it from search engine results; (2) withhold any financial revenue the web site may receive by preventing financial web sites from paying the site, as well as preventing advertisers from paying the site; and (3) remove the web site from search engines such as Google.

B. Stop Online Piracy Act (SOPA)[141]

SOPA is the House of Representatives' version of PIPA. SOPA borrows a number of provisions from PIPA, as well as adds language that goes beyond what is covered by PIPA.[142] Like PIPA, SOPA's target is "rogue" foreign web sites that infringe U.S. copyrights.[143] SOPA, however, contains an arguably broader definition of sites that are covered by using language such as "dedicated to theft of U.S. property."[144] Dedicated to the theft of U.S. property is further broken down: to fall within that category a site must (1) be in some way directed towards the United States and (2) either, "engage in, enable, or facilitate" infringement or take or have taken steps to "avoid confirming a high probability" of infringement.[145]

Another significant note is the changes SOPA would make to the DMCA takedown provisions. Under SOPA's notice and takedown provisions, copyright holders would be able to prevent payment sites and advertisers from working with an allegedly infringing site.[146] Therefore, while previously a web site could avoid liability by complying with a takedown notice, a web site under SOPA could face severe economic harm through the loss of advertising revenue in the interim while it takes actions to comply. SOPA also contains additional language that mandates "denying U.S. capital to notorious foreign infringers."[147] What constitutes a "notorious foreign infringer" is not defined, but the legislative language merely suggests that the Secretaries of Commerce and the Treasury should identify them.[148]

To summarize, PIPA and SOPA add a number of new tools and strengthen certain rights of copyright holders. In addition to the enforcement mechanisms available under current law, the two bills would add a few key tools. First, the bills provide a means for rights holders and the attorney general to filter a domain name to block users' access to it. Second, the bills provide a streamlined means of forcing a search engine to filter infringing links from its results. Third, the bills allow rights holders to bring actions to cut off online payment providers and

---

under PROTECT IP as the DMCA and therefore primarily covers search engines.

141. Stop Online Piracy Act, H.R. Res. 3261, 112th Cong. (as debated in the House Judiciary Committee and placed on hold by Rep. Lamar Smith on Jan. 18, 2012) [hereinafter SOPA].

142. *See id.*

143. *See id.*

144. *Id.* §§ 103–104.

145. *Id.* §§ 101(23), 103(a).

146. *Id.* § 102(b)(5).

147. SOPA, *supra* note 141, § 107.

148. *Id.*

advertising networks payments to alleged infringing sites. Fourth and finally, the bills significantly weaken the safe harbor provisions of the DMCA. The bills, of course, contain much more than these four elements, but these aspects are crucial to understanding their primary purpose.

C. Support and Opposition for PIPA and SOPA

PIPA and SOPA have proven to be incredibly polarizing. In the Senate, PIPA, which was introduced by Senator Patrick Leahy (D-VT), was co-signed by thirty-nine senators on both sides of the aisle.[149] In addition, the Chamber of Commerce, the Recording Industry Association of America, various entertainment industry associations, publishing companies, and a number of sports organizations support the bill.[150] From a business perspective the bill musters support due to the assumption that it will effectively reduce copyright infringement, and thus curtail the financial losses Congress believes piracy causes. It is interesting to note that on the congressional side there appears to be a general lack of knowledge as to what the bill would actually accomplish.[151]

Opponents of the bill include senators who feel that the bill will "trample" free speech and innovation.[152] For similar reasons, one of the largest trade associations in the realm of technology, the Consumer Electronics Association (CEA), has voiced its opposition to the bill, likening it to "killing the host to attack a parasite."[153] Large companies such as Google and Yahoo have also voiced their opposition due to the increased liability the bill would place on these companies.[154] Opposition from such companies is so strong that Yahoo left the Chamber of Commerce and Google has considered doing so over the Chamber's support for the

149. *Bill Summary & Status 112th Congress (2011–2012) S.968 Cosponsors*, THE LIBRARY OF CONGRESS (last visited Oct. 26, 2012) http://thomas.gov/cgi-bin/bdquery/z?d112:SN00968:@@@P.

150. Gaius Publius, *Who Supports SOPA & PIPA, the "Kill-the-Internet" Bills?*, AMERICABLOG (Dec. 27, 2011), http://americablog.com/2011/12/who-supports-sopa-pipa-the-kill-the-internet-bills.html; *SOPA (Stop Online Piracy Act) debate: Why are Google and Facebook against it?*, THE WASHINGTON POST (Nov. 17, 2011), http://www.washingtonpost.com/business/sopa-stop-online-piracy-act-debate-why-are-google-and-facebook-against-it/2011/11/17/gIQAvLubVN_story.html?tid=pm_business_pop.

151. *See* Mike Masnik, *Are There Any Politicians Who Know What PROTECT IP is about?*, TECH DIRT (July 19, 2011), http://www.techdirt.com/articles/20110718/15393615155/are-there-any-politicians-who-know-what-protect-ip-is-about-senator-hutchison-thinks-its-about-net-neutrality.shtml (describing senators who believe the PROTECT IP Act is about immigration, Internet kill switches, and net neutrality).

152. *See* Press Release, Sen. Wyden, Wyden Places Hold on Protect IP Act (May 26, 2011), http://wyden.senate.gov/newsroom/press/release/?id=33a39533-1b25-437b-ad1d-9039b44cde92.

153. Press Release, Consumer Electronics Association, CEA Emphasizes Innovation-Killing Nature of Pending Intellectual Property Legislation (Nov. 3, 2011), http://www.ce.org/Press/CurrentNews/press_release_detail.asp?id=12203.

154. *See* Jennifer Martinez, *Google Mulls Divorcing Chamber of Commerce,* POLITICO (Nov. 4, 2011), http://www.politico.com/news/stories/1111/67603.html.

bill.[155] Strong opposition to the bill comes from a group of 108 law professors who submitted a joint letter to Congress which argues that PIPA is arguably unconstitutional on First Amendment grounds, would create severe technical consequences affecting the security of the Internet address system, and will undermine U.S. foreign policy.[156]

Members of the technical community have also come out in opposition of the bill. Concerns have been raised about a number of issues created by the bill. For one, domain name filters could be easily avoided and worked around by users.[157] In addition, the DNS filter, like the type proposed by the Acts, would likely produce significant collateral damage, preventing users from accessing web sites that were not intended to be filtered.[158] Finally, the changes in the operation of DNS will create new security risks for individual users, banks, credit card web sites, and health care providers.[159] While the technical issues the bills create are not directly relevant to this Comment's analysis of the issue, the fact that the bill poses so many significant technical issues highlights the general lack of knowledge about what the bill would actually do.

SOPA has drawn a number of criticisms on its own, largely centered on the disruption it will cause to the DMCA. The language of SOPA's notice and takedown provisions drastically changes the dynamic of the current DMCA takedown regime by essentially shifting the burden from the copyright holder to the service provider. A service provider can no longer attempt to avoid liability by complying with notice and takedown provisions when it can be severely economically harmed *ex-ante*. SOPA includes language that will call into question thirteen years of court interpretation of the DMCA and its safe harbor provisions. It defines target sites as those "dedicated to theft of U.S. property."[160] This term is ill-defined in the statute and will need to be interpreted before its meaning is understood, much like the DMCA provisions the courts have been interpreting for years. In the meantime, if passed, then SOPA will place a number of sites that were built around DCMA compliance on questionable legal ground.

D. Current Status of the Bills

On January 16, 2012, thousands of web sites, including Wikipedia, Reddit, Twitter, and Google "blacked out" or posted a message in protest of the two

155. *See id.*

156. Professors' Letter in Opposition to "Preventing Real Online Threats to Economic Creativity and Theft of Intellectual Property Act of 2011" (July 5, 2011), http://blogs.law.stanford.edu/newsfeed/files/2011/07/PROTECT-IP-letter-final.pdf [hereinafter Law Professor Letter].

157. *See* Steve Crocker, David Dagon, Dan Kaminsky, Danny McPherson & Paul Vixie, *Security and Other Technical Concerns Raised by the DNS Filtering Requirements of the PROTECT IP Bill*, (May 2011), *available at* http://domainincite.com/docs/PROTECT-IP-Technical-Whitepaper-Final.pdf [hereinafter Whitepaper Technical Letter].

158. *Id.* at 13.

159. *Id.* at 10.

160. SOPA, *supra* note 141, § 103.

bills.[161] An estimated 160 million people viewed the blacked-out Wikipedia.[162] It marked the first day the two bills saw widespread coverage in the media. Three days prior to the blackout, plans were announced to remove the DNS filtering provisions from the bill.[163] In the days following the protest, opposition in the Senate rose to forty-five members up from twelve the day before the protest.[164] On January 20, 2012, a vote on PIPA was postponed.[165] The same day, House Judiciary Chairman Lamar Smith postponed any vote on SOPA after losing the support of a number of congressmen, including co-sponsors of the bill.[166] Both bills remain postponed while Congress further debates and discusses the legislation. The following Section will analyze the bills under current U.S. law, under international agreements and treaties, as well as from a policy perspective.

IV. ANALYSIS

A. Technological Infeasibility

Perhaps the most striking flaw of the two bills is the sheer number of technical issues. Perhaps these flaws are not surprising since a large number of senators who sponsored and debated the language of the bill have openly admitted or suggested that they do not fully understand how the Internet works and how the bills would interact with it.[167] There are three primary technical issues with the bills, which will be discussed in turn below.

1. Domain name system filtering

The first major technical issue is the enforcement of the bills through the use of the domain name system (DNS). The DNS system is considered a core protocol

161. *See Sopastrike.com*, SOPASTRIKE BLOG (Sept. 25, 2012, 10:45 AM), http://sopastrike.com/on-strike/ (showing a full list of web sites that participated in the protest against the Stop Online Piracy Act).

162. *See Wikipedia's Wales Says Blackout Worked*, REUTERS (Jan. 20, 2012), http://in.reuters.com/video/2012/01/20/wikipedias-wales-says-blackout-worked?videoId=228887329.

163. *See* Greg Sandoval, *DNS Provisions Pulled From SOPA, Victory For Opponents*, CNET (Jan. 13, 2012), http://news.cnet.com/8301-31001_3-57358947-261/dns-provision-pulled-from-sopa-victory-for-opponents.

164. *See* Grant Gross, *Internet's Protest Prods US Senate to Delay Vote,* PC WORLD (Jan. 20, 2012), http://www.pcworld.com/article/248466/internets_protest_prods_us_senate_to_delay_vote.html.

165. *Id.*

166. CBS News Staff, *SOPA is Dead, Smith Pulls Bill*, CBS NEWS (Jan. 20, 2012), http://www.cbsnews.com/8301-501465_162-57362990-501465/sopa-is-dead-smith-pulls-bill/.

167. *See* Alexandra Petri, *The Nightmarish SOPA Hearings*, WASH. POST (Dec. 15, 2011), http://www.washingtonpost.com/blogs/compost/post/the-nightmarish-sopa-hearings/2011/12/15/gIQA47RUwO_blog.html (quoting senators making a range of statements such as "I'm no tech expert," "I'm not a nerd," and "I have rarely been a part of a committee operation were we have not had . . . technical experts to deal with major concerns that have arisen").

on which the Internet is built.[168] All web sites are stored on web servers that are assigned an IP address.[169] An IP address is a number assigned to the site. For example, Facebook's IP address is 69.63.189.16.[170] A user can type that number into his browser and he will be brought to Facebook's site. Since a random string of numbers is difficult to remember, most Internet users access web sites via domain names.[171] The domain name system allows a user to type in a name followed by what is known as a top level domain such as ".com" or ".org."[172] This then directs the web browser to the appropriate IP address of the web site.[173] A domain name itself is distinct from the actual web site, which is stored on a computer server.[174] The domain is simply an address that allows the user to find the site.[175] A web site can have a number of domain names associated with it, all directed to the same page.

Under SOPA and PIPA, sites that are determined or alleged to be infringing could have their domain names filtered. The practical effect is that a domain name will not redirect a user to the appropriate web site. For the average user, the site will appear to have vanished from the Internet.[176] This is not entirely accurate as the site will still exist on a server and at its IP address, but the site will be inaccessible from that domain name.[177] This type of filtering is problematic for a number of reasons.

2. Security concerns

The second technical concern is security related. Increases in security threats such as web site spoofing to phish for user information[178] and redirecting users to fake web sites by hijacking the DNS lookup process has given rise to new security measures such as DNS Security Extension (DNSSEC). DNSSEC digitally "signs" data to ensure a user it is authentic.[179] This process monitors each step in the DNS

168. Whitepaper Technical Letter, *supra* note 157, at 3–4.

169. For a detailed explanation of how IP addresses work, *see Understanding TCP/IP Addressing and Subnet Basics*, MICROSOFT (Sept. 23, 2011), http://support.microsoft.com/kb/164015.

170. Bradley Mitchell, *What is the IP Address of Facebook?*, ABOUT.COM, http://compnetworking.about.com/od/traceipaddresses/f/facebook-ip-address.htm.

171. Marshall Brain & Stephanie Crawford, *How Domain Name Servers Work*, HOWSTUFFWORKS, http://www.howstuffworks.com/dns.htm.

172. *Id.*

173. *Id.*

174. *Id.*

175. *Id.*

176. *See* Matthew Lasar, *DNS Filtering: Absolutely the Wrong Way to Defend Copyrights,* ARS TECHNICA (July 2011), http://arstechnica.com/tech-policy/news/2011/05/dns-filtering-absolutely-the-wrong-way-to-defend-copyrights.ars (explaining how DNS filtering would work under SOPA).

177. *See* Brain, *supra* note 171.

178. An example of a "spoofed" web site is a site that appears to be an official web site of a bank or credit card company, but is actually operated by someone hoping to record users' login information and passwords which the customer enters believing the site is their banks web site.

179. *DNSSEC: What Is It and Why Is It Important?*, INTERNET CORPORATION FOR

lookup process to ensure that users are being directed to the sites they believe they are accessing. DNSSEC is a critical security measure that addresses one of the primary techniques hackers use to obtain passwords, financial information, and other confidential information.[180]

The DNS filtering components of PIPA and SOPA are at odds with this system because the U.S. government, much like a hacker or malicious program on a user's computer, would redirect a user that enters the domain name of a seized web site to a text page of the U.S. government stating that the web site has been seized. Experts suggest that implementation of both the DNSSEC security measures and the DNS filtering included in the bill is simply not possible.[181] For the bills' filtering requirements to function properly, DNSSEC must not be permitted to be implemented as an obstacle.

3. Work-arounds and circumvention

The third concern is that it is very easy for a user to work around a filtered domain. There are a number of methods that even a fairly casual Internet user can utilize. The first method is rather simple: a user can simply type the IP address of the web site into his browser.[182] The addresses are relatively easy to find through a quick Google search. In fact, there are browser add-ons that users can install to automate the process for them.[183] Second, users can use a proxy server located outside the United States to access a blocked site.[184] A proxy server essentially routes a user's traffic through a secondary location.[185] This allows the user to connect to the Internet from that location. Since SOPA and PIPA will only block web sites for U.S. users, a user could simply use a proxy located in a foreign country to access the sites.

In addition to the use of work-arounds by individual Internet users, web sites and businesses could navigate around the bills' restrictions as well. A company that wants to operate outside the reaches of SOPA could simply move offshore, and web sites could use offshore DNS providers not subject to U.S. law.[186] Some

---

ASSIGNED NAMES AND NUMBERS (Oct. 9, 2010), http://www.icann.org/en/announcements/dnssec-qaa-09oct08-en.htm.

180. Whitepaper Technical Letter, *supra* note 157, at 5.

181. *Id.*

182. *See* Brain, *supra* note 171.

183. *See The Pirate Bay Dancing Add-On Kills DNS and IP Blockades*, TORRENT FREAK (Nov. 30, 2011), http://torrentfreak.com/the-pirate-bay-dancing-add-on-kills-dns-and-ip-blockades-111130/.

184. *See* David Wang, *What is a DNS Block and 3 Ways to Get Around It,* ADVENTURES OF A BLOG JUNKIE (Sept. 25, 2012, 10:45AM), http://blogjunkie.net/2011/06/get-around-dns-block-filter.

185. *Id.*

186. Declan McCullugh, *OpenDNS: SOPA Will Be "Extremely Disruptive" to the Internet*, CNET (Nov. 17, 2011), http://news.cnet.com/8301-31921_3-57327341-281/opendns-sopa-will-be-extremely-disruptive-to-the-internet/.

companies have already considered this option.[187] This would of course, create an incentive for new companies to form outside the United States.[188]

This same principle applies to illegal sites. A seized web site can simply register a new domain name outside the United States and users can access the same content. In the case of the seized domain name rojadirecta.com, a new domain name, rojadirecta.es, was registered, and traffic from users reached the levels of the old site very quickly.[189] Offshore DNS providers potentially expose a user to security threats as well. A server may, and in fact would likely, be run by a "rogue" pirating or hacking group that has incentive to steal user information that passes through its server.[190] In addition to these quick work-arounds, the sheer volume of sites hosting or linking to infringing content makes individual domain seizures ineffective. For every site shutdown there are many more that users can go to for the same content.

Proponents of the bill argue that the ease of circumvention is not a significant issue. The proponents argue that just as a speed bump is easily avoided or a locked door can quickly be unlocked by someone with the right skills, the fact that it is easy to work around is not a reason not to do it. Casual users will be deterred, the argument follows. This argument has an interesting premise but is only compelling if the harm in implementing a measure that has minimal deterrent value is low. In the case of PIPA and SOPA, it is a difficult case to make, as the security issues alone seem to be enough to outweigh the minimal deterrent value the bills might have. From a technical standpoint, the solutions PIPA and SOPA pose to copyright infringement compromise important Internet security protocols in favor of an easily circumvented and questionably effective DNS filtering system.

B. Censorship, First Amendment, and Due Process Concerns

By using DNS filtering, SOPA and PIPA have the practical effect of removing web sites from the Internet for average users.[191] These provisions allow filtering to occur *ex parte*, with the accused web site not being represented.[192] This is because the bill would treat a domain name as a piece of real property and allow actions *in rem* to seize the property.[193] The bills do allow a site owner to challenge such a seizure but require that to do so, the owner must submit to U.S. jurisdiction.[194] By filtering entire web sites, the government is undoubtedly

187. *Id.*

188. *See infra* text accompanying notes 209–10.

189. Whitepaper Technical Letter, *supra,* note 157, at 7.

190. *Id.* at 11.

191. See *supra* section IV.A.1. for a description of the DNS filtering mechanism and how it blocks web site access for typical users.

192. SOPA, *supra* note 141, § 102(b)(2) (allowing *in rem* proceedings without the presence of the accused when the Attorney General is unable to locate the accused after searching with due diligence).

193. See *supra* notes 102–07 and accompanying text for a discussion about *in rem* jurisdiction and its application to domain names.

194. *See* SOPA, *supra* note 141, §102(c)(4)(C) (providing an affirmative defense only where the accused is subject to *in personam* jurisdiction).

removing protected speech from the Internet, as most web sites contain much more than infringing material.[195]

Constitutionally, speech is a highly protected right, and the suppression of it is allowed only in a narrow set of circumstances. Additionally, the Constitution requires that "a court, before material is completely removed from circulation . . . make a final determination that material is [unlawful] after an adversary hearing."[196] Any restrictions on free speech must be the "least restrictive means of advancing a compelling state interest."[197] Courts have found in the case of DNS filtering this means whenever a filter blocks a web site that hosts sub-pages under a single domain, it is unconstitutionally "overblocking."[198]

SOPA and PIPA do not require adversarial hearings prior to the seizure of a web site, but instead allow seizure immediately, before the investigation and determination of infringement.[199] This could have the effect of suppressing vast amounts of free speech because a large number of web sites host sub-web sites under the same domain. The suppression of the top web site would suppress many web sites that may not contain any illegal content but contain significant amounts of speech in the form of comments and user posts in forums.[200]

The bill allows a rights holder to block a payment provider or advertising network from doing business with the site,[201] raising serious due process concerns. This process occurs before any judicial hearing or other process involving the alleged web site has occurred.[202] The process has been described by one commentator as "not law—it's a kind of thuggery."[203] The only recourse a site faced with the cut off of its financial resources has is to submit to U.S. jurisdiction (which a court might not otherwise have) and challenge the action.[204]

Proponents of SOPA and PIPA argue that the primary targets of these bills are

---

195. For example, a seizure of youtube.com for a single infringing video would block access to hundreds of thousands of legitimate, user-made videos.

196. Ctr. for Democracy & Tech. v. Pappert, 337 F. Supp. 2d 606, 657 (E.D. Pa. 2004) (applying First Amendment free speech rights to the complete restriction of materials not yet determined to be illegal child pornography).

197. ACLU v. Ashcroft, 322 F.3d 240, 251 (E.D. Pa. 2004), *aff'd*, 542 U.S. 656 (2004).

198. *Pappert*, 337 F. Supp. 2d at 633–34.

199. *See* SOPA, *supra* note 141, § 102(b)(5) (allowing injunctive action against the site or site owner upon commencement of the action).

200. Law Professor Letter, *supra* note 156, at n.6.

201. SOPA, *supra* note 141, § 102(c)(2)(C).

202. *See* David Post, *Stopping the Stop Online Piracy Act*, VOLOHK CONSPIRACY (Dec. 4, 2011, 6:59 PM), http://volokh.com/2011/12/04/stopping-the-stop-online-piracy-act/ ("SOPA establishes a 'notice and take-down' scheme under which an IP rights holder need only notify banks, credit card companies, Internet advertisers, and Internet search engine operators, in writing, that he/she has a 'good faith belief' that an identified Internet site is 'primarily designed or operated for the purpose of' infringement.").

203. *Id.*

204. *See* SOPA, *supra* note 141, § 102(c)(4)(C) (providing an affirmative defense only where the accused is subject to *in personam* jurisdiction).

foreign web sites.[205] These web sites are usually owned by foreign citizens.[206] As non-citizens, the argument goes, they do not have constitutional rights when in an American court.[207] On its face this argument sounds compelling, but it has a number of flaws. First, assuming for the sake of argument that the Constitution does not apply to non-citizens in U.S. courts, the bill still runs afoul of constitutional rights of U.S. citizens who may operate a site.[208] While the bills may be targeted at the ill-defined "foreign rogue web sites," there is nothing that would prevent it from being applied to U.S. web sites as well. A rational copyright holder would not bring claims only against foreign sites and not U.S. sites infringing the same content. Assuming that the Constitution does not apply to non-citizens only addresses the due process concerns. A web site and its owners may be foreign, but blocking access to it could easily suppress the speech of American citizens using the site if the site allows user-generated content or includes a message board of some kind.

C. International Concerns

This type of filtering and censoring creates an interesting dilemma for the United States on the international scene.[209] The United States has long been a proponent of the free Internet, criticizing regimes such as China and Egypt for filtering and blocking access to it.[210] These acts would go further than even Internet censorship in China.[211] Commentators have noted that this kind of filtering of the Internet is "ironic" and compromises the ability of the United States to defend the notion of a free and open Internet globally.[212]

In addition to the bad message this type of legislation would send in regards

---

205. *See* Video Tape: Debate on The IP Wars: SOPA & PIPA: Strengthening Legitimate Protections for Rights Holders Or an Attack on the Internet?, held by Temple University Beasley School of Law (Jan. 31, 2012) (on file with Temple University); *see also* Mark Lemley, David Levine & David Post, *Don't Break the Internet*, 64 Stan. L. Rev. Online 34 (Dec. 19, 2011), http://www.stanfordlawreview.org/online/dont-break-internet (explaining that, while many of the provisions of SOPA and PIPA are applicable to any domain, some provisions are directed solely at domains operated by individuals outside the United States) [hereinafter *Don't Break the Internet*].

206. *See id.* ("These orders can be issued even when the domains in question are located outside of the United States . . . [and the] operators are themselves located outside the United States.").

207. *Id.*

208. *Id.*

209. *See id.* (describing how SOPA and PIPA represent a step towards the very Internet censorship that the United States has criticized as "a new information curtain [that] is descending across much of the world.").

210. *See, e.g.*, Hilary Rodham Clinton, Sec'y of State, Remarks on Internet Freedom (Jan. 1, 2010) (asserting the virtues of the Internet flow of information and criticizing many countries, including China and Egypt, for their efforts to stem that flow).

211. *See* Law Professor Letter, *supra* note 156, at 6 (noting that "even China doesn't demand that search engines outside China refuse to index or link to other Web sites outside China.").

212. *Don't Break the Internet*, *supra* note 205.

to filtering and blocking access to the Internet, the bill also sends the message that the United States will act unilaterally on international copyright matters and not work with other TRIPS parties or the WTO to solve an issue that is clearly global in nature. This sets a bad precedent. If the United States demonstrates a willingness to act unilaterally in these matters, China or any other WTO country may do so as well.

1. Impact on innovation and startups

An often cited effect of this type of legislation is the negative impact it will have on technology startups and Internet innovation.[213] The primary concern is the potential liability PIPA and SOPA would place on web sites that currently fall under safe harbor provisions in the DMCA.[214] As described in detail above, under current law, user-generated content sites such as YouTube are not responsible for the content their users upload outside of notice and takedown compliance.[215] Sites are not required to police themselves for copyright-infringing content.[216] Indeed, this type of policing on a site such as YouTube, where users upload thirty-five new hours of video every minute,[217] would be impossible. Sites simply do not have the ability to control what users upload before they upload it; yet, under PIPA and SOPA, they could potentially face being shut down or having advertising revenue frozen while the issue is resolved. This potential liability could deter many potential Internet startups from forming in the United States. It is therefore likely that sites will instead incorporate offshore because they will face less liability outside the United States. User-generated content sites are some of the most popular, innovative, and successful sites on the Internet, and U.S. companies are responsible for most of these sites.[218]

213. *See, e.g.*, *Growing Chorus of Opposition to "Stop Online Piracy Act"*, Center for Democracy & Technology (Jan. 9, 2012), https://www.cdt.org/report/growing-chorus-opposition-stop-online-piracy-act.

214. *See id.* (quoting Casey Rae-Hunter, *Online Piracy Bills are Flawed*, THE HILL (Jan. 4, 2012), *available at* http://thehill.com/blogs/congress-blog/technology/202311-online-piracy-bills-are-flawed) (reporting concerns that SOPA would force platform sites to self-censor in order to avoid liability). See *supra* Sections II.B.2–3 for a detailed explanation of the DMCA and its safe harbor provisions.

215. See *supra* notes 81–91 and accompanying text for the details of how the DMCA relieves web sites of responsibility for the content of user-generated posts.

216. *Id.*

217. Alison Diana, *YouTube Uploads 35 Hours of Video Every Minute,* INFORMATION WEEK (Nov. 12, 2010), http://www.informationweek.com/news/infrastructure/traffic_management/228200838.

218. *See Top Sites*, ALEXA, http://www.alexa.com/topsites/global (last visited Oct. 23, 2012) (listing the most popular web sites on the Internet).

D. Alternatives, Solutions, and Going Forward

1. How much damage is being done?

Before discussing alternatives and solutions, it is important to look first at the nature and scope of the problem. The issues of piracy, its effect on the content industry, and its seriousness are not generally the focus of the debate over SOPA and PIPA. Opponents of the bill will often acknowledge that they believe piracy is an acute problem and that they are merely arguing that SOPA and PIPA are not the proper solution.[219] The question of the extent and seriousness of piracy, however, should not be dismissed outright, as the question is far from settled.

The content industry suggests that every year, 750,000 jobs and $200 billion are lost to online piracy of copyrighted content.[220] The Government Accountability Office (GAO) has found that these numbers cannot be substantiated as no underlying study has been done.[221] The copyright industry itself reports that it outpaces the rest of the economy in real growth, that it pays its workers higher than average salaries, and that the copyright industry is a "key engine of growth for the U.S. economy."[222] It is unclear what kind of impact piracy is having. On the one hand, the copyright industry appears to be strong and thriving. On the other hand, it is possible that piracy has prevented even further growth in the industry.

When Megupload.com was recently shut down and its owners arrested, it was estimated that the total cost of its copyright infringement was in excess of $500 million.[223] This number was presumably generated by multiplying the value of each infringed file by the number of times it was downloaded, thus generating a number that in theory would show loss in sales. This figure relies on the assumption that every individual download of the content was a lost sale. That is to say, the person would have purchased the content if it was not available to download illegally. The problem with this assumption is that, of course, it may not be true that each individual who downloads copyrighted content would have bought that content otherwise.

Some content producers suggest that piracy might actually help them. Mikael Hed is the CEO of Rovio Mobile, the creator of the popular mobile phone application, Angry Birds. He believes that piracy of his game has helped him by drawing attention to his brand and often turning persons that would not be paying

---

219. *See e.g.*, *Don't Break the Internet*, *supra* note 205 (noting that, while "[c]opyright and trademark infringement on the Internet is a very real problem," PIPA and SOPA are not the right solution).

220. Brad Plummer, *Is Online Piracy a Big Problem? Evidence is Scant,* WASH. POST (Nov. 11, 2011), http://www.washingtonpost.com/blogs/ezra-klein/post/does-online-piracy-cost-jobs-its-hard-to-find-evidence/2011/11/04/gIQAVlH6lM_blog.html.

221. *Id*.

222. Steven E. Siwek, *Copyright Industries in the US Economy: The 2011 Report*, 2, 15, (Nov. 2011), http://www.iipa.com/pdf/2011CopyrightIndustriesReport.PDF.

223. David Kravets, *Megaupload Server Purge Delayed,* WIRED MAGAZINE (Jan. 31, 2012), http://www.wired.com/threatlevel/2012/01/megaupload-server-purge/.

customers at first into ones that are willing to pay for content in the future.[224] Like the claims of the copyright industry, Rovio Mobile's claim is difficult to back up with hard data, but it highlights the fact that it is far from clear what kind of harm piracy does.

With the unsettled question of piracy's effects and the uncertain status of SOPA and PIPA in mind, this Section looks at alternatives and potential solutions to the problem. It is clear from the prevalence of piracy and the ease with which it can be done that no single, simple solution will solve the problem. If defeating piracy is even possible, then a careful mix of policy, legislation, and international cooperation is needed to truly combat the threat.

2. Strengthening international agreements through the WTO

Piracy is clearly an international problem since a significant portion of it now occurs via the Internet. Despite this, there has been little to no discussion of an international solution to the problem. Bills like SOPA and PIPA create entirely unilateral solutions. International discussion of the issue, however, is extremely important.

The issue in many cases is that foreign countries and the United States disagree as to what constitutes infringement. The *Rojadirecta* case is an excellent example of this. Spanish courts decided twice that by providing links to sites that streamed copyright-infringing content, the web site itself was not infringing.[225] Under U.S. law, however, the web site faced liability by inducing infringement.[226] This type of discrepancy in the laws of the two countries creates serious issues for web sites that operate globally.

The Berne Convention and the TRIPS Agreement have created a strong framework for international copyright protection, but as discussed above,[227] they are not perfect. Specifically, the enforcement procedures are broad and general, and do not provide clear-cut standards for enforcement mechanisms.[228] One potential solution is to tighten these provisions and create standardized definitions by which all signatory countries must abide. Narrowing the provisions would provide each individual country less flexibility in enforcing copyright laws but would provide more predictability for copyright holders as well as web sites hosting content. With narrower performance standards and agreed-upon

224. Dragos Pirvu, *Rovio Mobile CEO: Piracy Is Not A Bad Thing, It Allowed Angry Birds To Grow Its Fanbase,* TECH SOURCE (Jan 31, 2012), http://www.tech.sc/rovio-mobile-piracy-is-not-bad-angry-birds-fanbase/.

225. Memorandum of Points and Authorities in Support of Claimant's Motion to Dismiss at 14, U.S. v. Rojadirecta.org, 11 Civ. 4139 (S.D.N.Y. 2011).

226. Government's Memorandum of Law In Opposition to The Motion By Claimant Puerto 80 Projects, S.L.U. to Dismiss the Verified Complaint at 18, U.S. v. Rojadirecta.org, 11 Civ. 4139 (S.D.N.Y. 2011).

227. See *supra* notes 108–15 and accompanying text for a detailed discussion of the Berne convention and the TRIPS agreement.

228. *Id.*

definitions, member countries could have a vastly more effective enforcement mechanism with which to hold each other accountable. The United States could handle a "rogue" web site operating in China by using the TRIPS enforcement mechanism to force China to take action. This removes any questions of extraterritoriality from the equation and allows an international body to compel domestic action from countries in violation of the standards.

However, the WTO is a difficult organization in which to make rules. With 160 nations, it is difficult to reach consensus, and many countries, such as China, may not favor stricter standards. Alternatively, enhanced enforcement mechanisms could be agreed upon in the U.N. through the WIPO, where such agreements could be easier to negotiate.

3. Domestic legislation that embraces international solutions

Another potential international solution is found in the Online Protection & Enforcement of Digital Trade Act (OPEN Act) drafted by Senator Ron Wyden (D-OR) and Representative Darrell Issa (R-CA).[229] In addition to providing a narrow definition of "rogue web site"[230] and removing the DNS and search engine provisions of SOPA,[231] the OPEN Act would allow copyright holders to petition the International Trade Commission (ITC) in much the same way as patent holders.[232] The ITC would investigate petitions to determine if the site meets the definition of a rogue web site.[233] Under the Act, a rogue web site must (1) have a non-domestic domain name; (2) conduct business in the United States; and (3) "[have] only limited purpose or use other than engaging in infringing activity and [an] owner or operator [who] primarily uses the site to willfully engage" in infringing activity.[234] Upon a determination from the commission that the web site is "rogue," the site will be required to cease its conduct, and the copyright holder can take the decision of the ITC to online payment providers and advertising networks and have them cut off funds to the site.[235] The Act also provides an opt-out provision that allows a foreign web site to waive the ITC investigation and decision by submitting to U.S. jurisdiction.[236] This approach places an international

229. H.R. 3782, 112th Cong. (2012) [hereinafter OPEN]; *see also* The Office of Congressman Darrell Issa, *OPEN: Online Protection and Enforcement of Digital Trade Act*, KEEPTHEWEBOPEN (last visited on Oct. 24, 2012), http://keepthewebopen.com/open-archive (providing a draft of the OPEN Act that is open for comments).

230. *See* OPEN, *supra* note 229, § 337A(a)(8) (defining "Internet Site Dedicated to Infringing Activity").

231. *See id.* § 337A(d) (establishing a complaint process that does not include DNS interference).

232. *See id.* §§ 337A(d) (establishing a complaint process that allows complainants to file suit with the International Trade Commission).

233. *Id.* § 337A(b).

234. *Id.* § 337A(a)(8).

235. Eric Goldman, *The OPEN Act: Significantly Flawed, But More Salvageable Then SOPA/ PROTECT IP*, ARS TECHNICA (Jan. 1, 2012), http://arstechnica.com/tech-policy/news/2011/12/the-open-act-significantly-flawed-but-more-salvageable-than-sopaprotect-ip.ars.

236. *Id.*

organization between a web site and a foreign government or rights holder, providing more legal process. This approach would help ease concern over unilateral action taken by the United States.[237]

4. Innovation by affected industries

Stronger domestic and international protections can only go so far in fighting piracy. The Internet has truly revolutionized the way media is distributed and consumed. Many content industries have handled this well. As Valve CEO, Gabe Newell, argues, much, but not all, of online piracy has to do with convenience and service, and not with pricing.[238] Valve, a company that produces computer games, confronted the piracy problem by creating Steam, an online platform where users can purchase and download games directly.[239] Using its convenient and simple digital distribution program, Valve has had great success in decreasing piracy of its games and capturing huge markets like Russia, where piracy was once rampant.[240]

Apple has also had immense success in utilizing convenience to combat piracy. Amidst the Napster copyright litigation of the early 2000s,[241] Apple released iTunes 4, a music player that enabled users to directly download individual songs for ninety-nine cents each.[242] By negotiating agreements with record companies, Apple offered to them a new means of distributing music to customers that was far more convenient than going to the store. Upon its release, "iTunes Music Store brought 200,000 high-quality songs from BMG, EMI, Sony Music Entertainment, Universal and Warner under one fully searchable, completely legal roof."[243] iTunes sold one million tracks in the first week alone and surpassed ten million downloads within four months.[244] By offering consumers a convenient, legal, and affordable means of purchasing music, Apple and iTunes played a significant role in the continued success of the music industry.[245]

---

237. It should be noted that OPEN is not a perfect solution as it currently stands; however, it does address many of the concerns voiced by SOPA and PIPA critics. Critics of OPEN suggest that the bill may still encourage many companies, specifically, advertising networks, to shift overseas, draw issue with the use of the ITC, and believe that its definitions are still too vague. For an overview of these arguments, see *id.*

238. Interview with Gabe Newell, Co-founder and CEO, Valve (Nov. 24, 2011), http://www.tcs.cam.ac.uk/story_type/site_trail_story/interview-gabe-newell/ ("[W]e think there is a fundamental misconception about piracy. Piracy is almost always a service problem and not a pricing problem.").

239. *Id.*

240. *Id.*

241. See *supra* notes 60–72 and accompanying text for a detailed discussion of the litigation against Napster and other P2P sharing programs.

242. Michael Simon, *The Complete iTunes History – SoundJam MP to iTunes 9*, MACLIFE (Sept. 11, 2009), http://www.maclife.com/article/feature/complete_itunes_history_soundjam_mp_itunes_9 (opining that, without iTunes, the music industry would not have recovered from MP3 piracy).

243. *Id.*

244. *Id.*

245. *See* Ed Nash, *How Steve Jobs Saved the Music Industry*, WALL ST. J. (Oct. 21, 2011),

The successes of these companies show that a solution to piracy does not necessarily need to be legislation. Companies and industries that can innovate along with the Internet and embrace the change it has forced onto many industries can be highly successful.

V. CONCLUSION

Global online piracy and copyright infringement is a significant international issue. Some of the largest industries in the United States rely on the strong and effective enforcement of their intellectual property rights to succeed. The United States, through the DMCA and international agreements such as TRIPS, has long provided copyright holders with effective means of combating online copyright infringement. As new piracy threats emerge, particularly overseas, and calls for new enforcement mechanisms are made, the government and legislature need to carefully consider new means of enforcement.

In considering new intellectual property legislation, the legislature needs to consider the value of what it is protecting, the effectiveness and feasibility of the measures it seeks to implement, the harm or collateral damage that such measures will cause, and the international community within which it operates. SOPA and PIPA are not products of careful consideration of these factors. Moving forward, the most sensible solution is to slow down and rework any legislation with carefully thought out and narrow definitions, consider the balance between the rights of copyright holders and the rights of Americans to a free and open Internet, and reach out to the international community in crafting a solution.

http://online.wsj.com/article/SB10001424052970204002304576629463753783594.html.