Intellectual Property Brief

Volume 2
Issue 1 *Summer 2010*

Article 5

1-1-2010

Policing the Information Super Highway: Custom's Role in Digital Piracy

Andrew Haberman

Policing the Information Super Highway: Custom's Role in Digital Piracy

Keywords
Web technology, International marketplace, Internet, Internet piracy, Copyright, copyright rights, Immigration and Customs Enforcement ("ICE"), Intellectual property infringement

Policing the Information Super Highway: Customs' Role in Digital Piracy

By Andrew Haberman

I. Introduction

As the role of web technology and instant viral communication has permeated almost all sectors of commerce and consumer daily life, some great advantages have been dealt throughout the international marketplace.[1] While the Internet's economic necessity is evident in a business's ability to reach consumers and increase the efficiency of workflow, the duality of this new tool is evident in the problems of security and piracy. The profound effect on individual consumers is clear when one considers the role of purchase power online. Whereas in earlier decades consumers might have been limited by location, availability and ability to price out all of their options or opportunities to find what they want, the Internet has completely decimated this information and logistical economic block. Today anyone can look virtually anywhere to find virtually anything on the virtual marketplace of the web, shifting the economic power from the sellers to the masses. This shift is exacerbated by the increased competition that pirated goods play in this new unregulated market. As the world has entered the digital age, so too have pirates, and this poses a major obstacle to companies who build their business model around intellectual property. The prevalent availability of infringing goods, simplicity of acquiring these goods, and shroud of anonymity provided by the Internet to the seller makes the Internet a major obstacle for businesses in the digital age. This infringing material can come from anywhere in the world, and there is no easy solution to this ubiquitous and expanding problem.

In order to stem the growth of Internet piracy, the United States must begin to protect its citizens and businesses from pirated material, commencing with the Department of Homeland Security's Bureaus of Customs and Border Protection ("CBP") and Immigration and Customs Enforcement ("ICE") taking a larger role in policing this offence at the United States' cyber borders.[2] This paper will argue that Customs must begin to work with internet service providers ("ISPs") in order to police digitally transferred pirated copyrighted goods. First, Part II will present a brief overview of how the Internet, copyright rights, and Customs' authority currently function. Next, Part III will argue that Customs has the statutory power to police the United States' "e-borders," that expanding Customs' role will be easier than having the judiciary resolve such disputes, and that allowing Customs to monitor cyberspace will achieve harmony with multinational and national efforts being made to stop digital piracy worldwide. Finally, Part IV will conclude that in an age of ever-evolving piracy, a combination of Customs enforcement and encryption technologies will enable the United States to battle pirates on what is and will continue to be a major source of intellectual property infringement.

II. Background

The Growth of the Internet and Piracy

On any given day, more than 1.8 billion people around the world use the Internet.[3] With the declining

1. *See* Bus. Software Alliance, Software Piracy on the Internet: A Threat To Your Security (2009), *available at* http://global.bsa.org/internetreport2009/2009internetpiracyreport.pdf (asserting that software and computers have become "indispensible tools in our businesses, school and personal lives").

2. *See* Tom Spring, *Surfing With U.S. Customs*, CNN.COM, Oct. 20, 1999, http://www.cnn.com/TECH/computing/9910/20/us.customs.idg/ (reporting that Customs' CyberSmuggling Center had only $2 million, or .14%, of Customs' $1.7 billion budget in 2000); *See generally* Andreas Manolopoulos, *Raising 'Cyber Borders': The Interaction Between Law and Technology,* 11 Int'l J. of L. & Info. Tech. 40-53 (2003).

3. *See Internet* World Stats, Internet World Stats: Usage and Population Statistics, *available at* http://www.internet

cost of computer technology and the expansive nature of its use, the Internet is rapidly growing. However, a large portion of this growth is occurring in countries with rampant piracy.[4] In fact, much of this growth has come in countries currently on the United States' Special 301 Watch List, indicating that these countries have done an insufficient job protecting intellectual property rights.[5] Although the Special 301 reports are not directly linked to Internet piracy specifically, there are indications that countries with expanding Internet use are significantly contributing to the growth of Internet piracy.[6]

The Internet, as it stands today, is an end-user driven technology: there are few "control points" where a private or governmental organization can monitor what material is being placed on the Internet.[7] However, ISP's, which allow users to access the Internet, do have the capabilities of viewing, monitoring, and even revoking a user's Internet access.[8] Since the Internet is an end-user driven technology, any user is free to create a website, whether for legal or illegal purposes.[9] While this has revolutionized the process by which legitimate goods and services are distributed throughout the world, it also allows any user to create a site to distribute or sell counterfeit goods. This has given rise to an infinite number of "businesses" who use the web as both a communications tool and a global marketplace for goods, in what is called e-commerce. Illegal "e-businesses" range from sites providing for the digital transfer of music and media to those allowing the purchase of blatantly counterfeit goods, such as copyrighted films on DVD. This widespread reality has also affected consumers who are unaware of where their funds go when they unintentionally purchase counterfeit goods over the Internet.

Piracy over the Internet occurs primarily in two forms. First, tangible goods are purchased over the Internet with electronically transferred funds, and then the goods are shipped to the consumer.[10] These goods range from illegal copies of goods protected by copyright (like movies or CDs) to pharmaceuticals which infringe American patents (like generic forms of Viagra). Second, an infringing good may be transferred digitally over the Internet through "digital piracy." There is no question that CBP may assert its authority over counterfeit goods shipped into the United States, regardless of how these good were purchased, but the second type of Internet piracy raises many more legal concerns.[11] Since the vast majority of patented and trademarked goods are physical and cannot be digitally transferred, digital piracy primarily concerns copyrights.[12] As such, the primary industries affected by strictly digital piracy are the entertainment and software industries.

The Rights of Copyright Holders

Since copyrights comprise the majority of the intellectual property illegally transferred over the Internet in digital piracy, it is important to understand the rights that copyright holders are afforded when they produce a work. First, in order to be afforded these rights, an author must create a work that is

worldstats.com/stats.htm.

4. *See Bus. Software Alliance, Sixth Annual BSA-IDC Global software 08 Piracy Study* (2009), *available at* http://images.autodesk.com/adsk/files/globalpiracy2008.pdf; Internet World Stats, *supra* note 3 (reporting user growth of 399% worldwide since 2000, with growth rates as large as 1,675.1% in the Middle East.)

5. *Compare* Office of U.S. Trade Representative, 2009 Special 301 Report (Apr. 20, 2009) (listing, among others China, Russia, Indonesia, Chile, and Pakistan on the Priority Watch List) *with* Internet World Stats, *supra* note 3 (calculating user growth at between 568% and 934% in the past decade for countries in the same regions).

6. See *Bus. Software Alliance, supra* note 4 (despite the drop in the rate of PC software piracy in 52% of the 110 countries studied, global piracy has increased, indicating that piracy is growing so quickly in some countries as to negate the progress made world-wide).

7. *See* Dan. L. Burk, *The Market for Digital Piracy in* Borders in Cyberspace: Information policy and the Global Information Infrastructure, 205-34 at 206-07 (Brian Kahin & Charles Nesson eds., MIT Press 1999) (describing how users communicate through digital data packet switching on the Internet and control their inputs).

8. Matt Jackson, *Providing Safe Harbors for Speech: Internet Service Providers and Copyright Law in* Intellectual Property and Information Wealth: Issues and Practices in the Digital Age, 307-320, at 307 (Peer K. Yu ed., Praeger 2007) ("[ISPs] are the intermediaries that connect users to the Internet, allowing individuals to communicate.").

9. *See* Burk, *supra* note 7 (describing the freedom users have on the Internet).

10. *See* Brooks Barnes, *Fox Files More Suits Claiming DVD Piracy*, N.Y. Times (Feb. 4, 2010) *available at* http://mediadecoder.blogs.nytimes.com/2010/02/04/fox-files-more-suits-against-alleged-dvd-pirates/ (filing suits against individuals selling pirated DVDs on auction sites); CpTech.org, *Priority Watch Country*: Jordan, *available at* http://www.cptech.org/ip/health/phrma/301-99/jordan.html (reporting Jordan's involvement in pirating pharmaceuticals).

11. *See* 17 U.S.C. §603(c) (2006) (giving Customs authority to seize piratical or possibly piratical copies).

12. *But see Bilski v. Kappos*, 561 U.S. 1, 3 (2010) (slip op.) (holding business methods patentable, and thus, increasing the amount of electronically transferable patents); *see also* Debora J. Halbert, Intellectual Property in the Information Age: The Politics of Expanding Ownership Right, at 51-56 (Quorum Books 1999) (documenting the classification of programs as creative works).

capable of being copyrighted.[13] This requirement is not very stringent and merely requires that the author has produced a work with a modicum of creativity that is fixed in some medium.[14] In digital context, this "fixation" requirement becomes a source of debate, but in the United States, digital files have been determined to be a fixation.[15] If an author creates a copyrightable work, the Copyright Act identifies the six exclusive rights of the creator as the rights to: reproduce, adapt, distribute, publicly display, and publicly perform a copyrighted work, along with, in the case of sound recordings, the right to perform the digital transmission publicly.[16] Further, the Digital Millennium Copyright Act ensures the "protection of copyright owners against the unauthorized access to their encrypted copyrighted works."[17] This makes the use of "circumvention devices" illegal.[18] Thus if anyone copies, adapts, distributes, displays, or performs a copyrighted work without a license to do so, they are guilty of copyright infringement and the copyright owner maintains the right to prosecute these offenses. For their part, ISPs have been given limited liability for any infringement occurring on their servers since they are not actually violating these rights.[19]

Industries built around copyright protection, such as the entertainment industry, are able to subsist because the authors of works control the aforementioned exclusive rights to their works. Copyrights are granted in order to reward authors for the hard work they have put into their work, whether they have put months of research and writing into publishing a book or millions of dollars into creating a new type of animation for filmmaking. Without these protections, anyone who so desired would be able to watch a copyrighted movie for free on the Internet, and the incentive to innovate, or even to produce works would be significantly decreased.[20] Movies like "Avatar",which employ cutting edge technology never before seen on a movie screen, would no longer be created, and the general public will suffer as a whole.[21] The movie, music, and software industries base their business models on copyright protections, and if these protections are not effectively enforced, the incentive to innovate is lost.

Customs' Authority

The Department of Homeland Security's Bureaus of Customs and Border Patrol ("CBP") and Immigration and Customs Enforcement ("ICE") protect against the importation of goods infringing intellectual property rights.[22] However, Customs faces a unique task in protecting copyrighted works, as these works are no longer required to be registered under the Berne Convention.[23] To combat this problem, Customs allows copyright holders to record their copyrights with Customs, which assists them in protecting the owner's intellectual property. Under their enforcement authority, Customs may seize any "clearly piratical works" or works that are "substantially similar" to a copyrighted work.[24] Customs will generally make decisions regarding the legality of an imported work independently, but if the Customs Office, the IPR

13. *See Feist Publications, Inc., v. Rural Telephone Service Co.*, 499 U.S. 340, 345 (1991) (allowing a copyright if the author showed some creativity, regardless of other works already granted copyrights).

14. *See* 17 U.S.C.A § 101 (2006) ("[a] work is 'fixed' in a tangible medium of expression when its embodiment in a copy or phonorecord, by or under the authority of the author, is sufficiently permanent or stable to permit it to be perceived, reproduced, or otherwise communicated for a period of more than transitory duration.").

15. *See* Tyler T. Ochoa, *Copyright, Derivative Works And Fixation: is Galoob A Mirage, or Does The Form(gen) of the Alleged Derivative Work Matter?,* 20 Santa Clara Comp. & High Tech. L J. 991 (2003-04).

16. 17 U.S.C. §106 (2006).

17. Pub. L. 105-304, Stat. 2860 §5(C) (1998) (codified in scattered sections of 17 U.S.C. at §1201).

18. *See id.*

19. *See MGM Studios, Inc. v. Grokster, Ltd.,* 545 U.S. 913, 927-28 (2005) (an intermediary cannot be held liable unless they knowingly contribute to infringement); *see also* Jackson, *supra* note 8 (noting that ISPs do not commit the infringement, but instead their users do, thus, if anything ISPs could be charged as secondarily liable).

20. *See* Halbert, *supra* note 13, at 26-27 (noting that the National Writers Guild identified Internet piracy as a problem that "must be dealt with before is safe for intellectual property"); Peter Sciretta, *The most Pirated Movies of 2009 and Avatar: The Making of Bootleg*, Slashfilm, Dec. 27, 2009, http://www.slashfilm.com/2009/12/27/the-most-pirated-movies-of-2009-and-avatar-the-making-of-the-bootleg/ (citing ChartsBin, Top 10 Most Pirated Movies of 2009, Jan. 2010, http://chartsbin.com/view/3w3) (showing highly pirated movies to be downloaded tens of thousands of times).

21. Michael Cieply, *A Movie's Budget Pops From the Screen*, N.Y. Times, Nov. 9, 2009 *available at* http://www.nytimes.com/2009/11/09/business/media/09avatar.html (questioning whether Avatar was capable of making back its money in the current entertainment environment).

22. See, e.g., 17 U.S.C. § 602-03 (2006) (copyright law) (providing statutory authority for CBP and ICE to protect copyrighted works from infringing imported works).

23. Berne Convention for the Protection of Literary and Artistic Works, 828 U.N.T.S. 221,§14 (1977).

24. *See* 18 U.S.C. § 1595 (a)-(b) (seizure authority for violations of 17 U.S.C. § 602(b) (copyright statue).

Branch, or the courts issue a ruling, Customs must abide by the decision.[25] In addition to the statutory language, Customs is guided by the Copyright Directive, which is used as a step-by-step guide by customs lawyers to enforce copyrights at the borders.[26]

By its own policy, Customs must follow a specific set of steps upon making a determination of copyright infringement.[27] First, Customs notifies the importer of the alleged infringement if they decide to detain an import. If the importer files a timely denial, Customs will then notify the copyright owner, and if the copyright owner files a written request asking for the materials to remain detained, the importer is afforded an opportunity to submit a brief on his or her behalf.[28] While Customs protects the U.S. from infringing works at the borders, ICE has statutory authority to commence criminal investigations for infractions of Title 18 criminal intellectual property infringement.[29] ICE may initiate a criminal investigation if they have probable cause to believe that a crime involving copyrights, such as willful infringement, has been committed under Section 2319. ICE works with the FBI, National IPR Center and the DOJ to prosecute criminal individuals or organizations "responsible for producing, smuggling, and distributing counterfeit products."[30]

III. Analysis

Although there are not statistics on the precise amount of losses as a result of digital piracy, it is clear that piracy has had an enormous effect on industries built around copyright protection.[31] The Business Software Alliance estimates that the software industry experienced $53 billion in losses worldwide in 2008, but this is not strictly limited to digital transfer.[32] Similarly, the recording industries have also experienced a flood of digital piracy and have engaged in a myriad of tactics to try to stop the piracy. First, the recording industry began suing end users who allegedly stole music.[33] However, this plan proved expensive, ineffective, and generally unhelpful. Instead the recording industry, represented by the Recording Industry Association of America ("RIAA"), has been attempting to negotiate with ISPs in order to find a more effective solution to halting digital piracy.[34] The RIAA has furthered these efforts by requesting subpoenas under the Digital Millennium Copyright Act ("DMCA") in a bid to seek out consumers suspected of using peer-to-peer file sharing technology for alleged copyright infringement.[35]

Private negotiations between the recording industry and the ISPs will most likely prove ineffective without government involvement. However, a solution involving Customs might be able to curb the problem by preventing infringing files from entering the United States, and importantly, there is no limiting statutory language to prevent Customs from getting involved. Customs involvement will also avoid the problems that copyright owners face in civil lawsuits and provide an impartial arbiter to ISP infringement determinations.

A. Customs Has the Authority to Seize Illegal Digital Transfers Entering the United States

Customs regulations define infringing copies as "piratical articles, i.e., copies or phonorecords which are unlawfully made (without authorization of the copyright owner)" and importation of these copies is prohibited.[36] There is nothing in these rules limiting a copy to a physical copy, and further, there is nothing limiting importation to a physical import. As stated in *Caminetti v. United States,* "[i]t is elementary that the meaning of a statute must, in the first instance, be sought in the language in which the act is framed, and if that is

25. *See* Timothy P. Trainer & Vicki E. Allums, Protecting Intellectual Property Rights Across Borders (ed. 2009) 448 (West 2009) (although there is no set analysis, Customs employs a quasi-judicial analysis in making infringement decisions).

26. See *id.* at 309-28 (supplying the text of the directive).

27. 19 C.F.R. 133.43 (2009); *See generally id.* at §133.43(b) (listing the information that must disclosed in each step of this process).

28. *See id* at §133.43(d).

29. *See* 18 U.S.C. §2319 (2006). *See also id.* §2318 (trademarks).

30. *See* http://www.ice.gov/pi/cornerstone/ipr/index.htm. While ICE's authority extends beyond the Internet, the National IPR focuses explicitly on Internet crimes and instead focuses on crimes with an international nexus, unlike the FBI. Due to the growth of cyber crime and Internet piracy, the DOJ has created the Computer Crime and Intellectual Property Section ("CCIPS") to handle the prosecution of these type of crimes. Thus, it is extremely important for these agencies to work together and share information while prosecuting cyber crime.

31. *See* Spring, *supra* note 2 (estimating that U.S. business lose $10 billion per year to computer related crime); Halbert *supra,* note 16 at 83 (Documenting the $1 billion sanction place on China in 1995 for failure to protect products ranging from *Disney's Lion King* to Microsoft's computer programs).

32. *See* Bus. Software Alliance, *supra* note 1 (reporting from a study on 110 countries).

33. *See* Sara Mcbride & Ethan Smith, *Music Industry to Abandon Mass Suits*, Wall Street Journal, Dec. 19, 2008 *available at* http://online.wsj.com/article/SB122966038836021137.html.

34. *See id.*

35. *See, e.g. RIAA v. Verizon Internet Services, Inc.* 351 F. 3d 1229 (D.C .Cir. 2003).

36. 19 C.F.R. §133.41(a), (b).

plain... the sole function of the courts is to enforce it according to its terms."[37] Since the natural meaning of "import" is "to bring from a foreign or external source", there is no reason to exclude digital transfers across cyber borders.[38] Similarly, the maxim *noscitur a sociis* requires that when a word is ambiguous, its meaning be determined by reference to the rest of the statute.[39] In this case, the word "copies" is as unknown, as the word "import," when the statue is read without reference to other documents. Since the courts have determined that a pirated song in a digital format can be an infringing copy, it should follow that importing an infringing digital file should qualify as an infringement.[40]

Although Customs is already spread thin in its efforts to enforce intellectual property rights and protect American borders, Customs should be able to utilize ISPs to ease the load. ISPs are capable of monitoring the Internet for infringing conduct and have been able to do so in the past.[41] Further, other countries have successfully implemented e-borders monitors for certain material, and although this may be simpler than patrolling for any infringing material, it proves that monitoring in some capacity is certainly possible.[42] For example, France has worked with ISPs to prevent French Internet surfers from accessing Nazi memorabilia on Yahoo!'s auction site, while China has been censoring the results of Google searches for Chinese users.[43] ISP monitoring can be supplemented by ICE investigations and will not only work to discourage digital piracy, but should also curb piracy in tangible goods by supplying ICE with tangible leads to piratical organizations.[44] Since the world is moving digital, this will finally allow customs to move ahead of pirates who employ sophisticated hacking techniques.

It is important to note that although a CBP monitoring system will be essential to preventing digitally pirated goods from entering the United States, additional ICE action will be crucial in enforcing intellectual property rights. Almost seventy-five percent of the pirated goods shipped into the United States as a result of an Internet transaction come from auction sites.[45] Auction sites attempt to implement monitoring systems, but it is very hard to determine which goods are infringing.[46] Even Customs' monitoring will be unable to detect when infringing products are sold while being advertised as legitimate, showing the need for traditional CBP and ICE border measures and investigations, respectively, to prevent infringing physical goods from entering the United States.

In order to truly comprehend the value of Customs' role in preventing digital piracy, it also critical to examine the proposed monitoring system's limitations. Two readily apparent limitations of such a plan are: (1) end-user's privacy concerns could limit the scope of monitoring; and (2) new pirating methods could render this enforcement method useless. Implementation of a monitoring system will require a careful balancing of privacy and copyright owners' rights, but there are some examples that can be looked to in achieving this balance.

For example, the courts have ruled that the FBI Carnivore program, which monitors web activity, is constitutional, and this logic could similarly be

37. 242 U.S. 470 (1917).

38. "Import." Merriam-Webster Online Dictionary.. Merriam-Webster Online, Mar. 23, 2010, http://www.merriam-webster.com/dictionary/import.

39. Arecki *v. G. D. Searle & Co.,* 367 U.S. 303, 307 (1961) (implementing *noscitur a sociis*, which literally means " [the] word is known by the company it keeps") .

40. *See, e.g.*, *A&M Records, Inc. v. Napster, Inc.*, 114 F. Supp. 2d 896 (N.D. Cal. 2000), aff'd in part, rev'd in part, 239 F.3d 1004 (9th Cir. 2001) (holding Napster liable for distributing digital copies of songs); *see also* Robert C. Piasentin, *Unlawful? Innovative? Unstoppable?: A Comparative Analysis of the Potential Legal Liability Facing P2P End-Users in the United States, United Kingdom, and Canada*, 14 Int'l J. L. & Info. Tech. 95 (2006).

41. *See* Martin Charles Gloumbic, Fighting Terror Online: The Convergence of Security, Technology, and the Law, *at* 148-149 (Springer 2008) (documenting monitoring software such as Echelon and sniffers like the Carnivore program which utilizes ISPs to monitor Internet activity for specific information it is programmed to look for).

42. *See id.* at 4-5 (pointing out the difference in a user's Internet experience in France, Korea, Italy and China).

43. *See LICRA v. Yahoo! Inc.* (County Court, Paris, Nov. 20, 2000, *available at* http:www.lapres.net/yahen11.html (prohibiting the sale of Nazi memorabilia oh Yahoo!'s website in France); The Official Google Blog, *A New Approach to China: Update*, March 22, 2010, http://googleblog.blogspot.cowm/2010/03/new-approach-to-china-update.html (announcing that Google removed monitors in response to cyber attack suspected to have originated from the Chinese government).

44. *See, e.g.*, Joseph W. Cormier et. al., *Intellectual Property Crimes*, 46 Am. Crim. L. Rev. 761 (2009) (noting that together Customs, the DOJ and the FBI, through the "Joint Piracy Initiative" and operations such as "Site Down" and "D-Elite" have already began cracking down on Internet piracy of copyrighted goods).

45. *See* Internet Crime Complaint Ctr., 2009 Internet Crime Report (Mar. 12, 2010) *available at* http://www.ic3.gov / media/annualreport/2009_IC3Report.pdf. (336,655 complaints and $559.7 million lost to internet crime in 2009).

46. *See* EBay,The Verified Rights Owner Program (VERO) , http://pages.ebay.com /tradingassistants/TA_Education_VERO.pdf (describing EBay's policy to remove infringing material).

applied to an ISP monitoring systems for Customs.[47] Although national security is of a higher social value than protecting the record and software industry, these industries are essential to the American economy and have become a major concern in American foreign policy.[48] Further, one can assume that if Customs starts to monitor e-borders, pirates will likely either find ways to circumvent this system or attempt new methods of piracy. For example, pirates could just pre-load iPods with thousands of pirated songs and movies, enter the United States, and distribute pirated materials this way.[49] Since this proposed system would not be able to combat piracy within the United States, physical transport of files into the United States would be able to circumvent the monitoring system. However, with the majority of piracy occurring in developing countries, this would be a step in the right direction towards preventing massive future piracy.[50] Monitoring ISPs for digital piracy would, at the least, begin to bring enforcement measures up to speed with the measures implemented by pirates and begin to solve the rampant problem of digital piracy.

The RIAA and Business Software Alliance ("BSA") both support a monitoring system that uses ISPs as a control point, but they both realize that this cannot be accomplished privately without eroding end-users rights.[51] Thus, Customs' involvement will give end-users due process and an impartial arbiter to determine if an end-user has truly infringed a copyright. Furthermore, neither the end-users nor the ISPs need to be punished, as infringing material can simply be seized and destroyed. ICE will be able to follow up and pursue any criminal sanctions while the RIAA pursues civil action, but if the industry can prevent piracy, it is unlikely the RIAA will sue when the rewards do not justify the costs.

B. Problems With Private and Judicial Solutions

By abandoning the strategy of suing individual copyright infringers and beginning to work with ISPs to monitor the Internet, the recording industry has shown the type of forward thinking that will be required to thwart digital piracy. However, the recording industry seemed to abandon this plan without an effective substitute in place. Copyright holders in all industries, including the recording industry, have attempted to slow piracy through Digital Rights Management ("DRM") but this technology has been of little obstacle for pirates.[52] Pirates are not just children sitting at their computers downloading a free song but are instead highly organized groups working to make movies, music, software and other digital files available for free on the Internet.[53] Pirates have consistently been either one step ahead or capable of circumventing technological safeguards such as DRMs and have left industries reliant on copyright protection grasping for answers.[54]

One possible answer is a private agreement which monitors end-user Internet activity and allows the record company to unilaterally shut down Internet service if infringement occurs. However, any such program will still require an accompanying civil lawsuit and will likely violate the constitutional freedoms of speech and privacy, especially without an impartial decision maker to determine when a user has acted illegally.[55] Second, it will be questionable if American courts can even establish jurisdiction, and if they can,

47. *See* Stephen A. Saltzburg & Daniel J. Capra, American Civil Procedure: Cases and Commentary, 52 (8th ed., Thompson West 2007) (1980) (noting that in "full collection" mode the Carnivore system violates the Fourth Amendment, but in "pen collection" mode, which can monitor file transfer, the system is constitutional under the USA Patriot Act).

48. *See id.* (noting that the Patriot Act was passed in response to September 11th). *But see Transcript, Barack Obama's Inaugural Address*, N.Y. Times, Jan. 20, 2009, *available at*: http://www .nytimes.com/2009/01/20/us/politics/20text-obama.html (showing the importance of science as President Obama stated, "We will restore science to its rightful place.").

49. *See* EConsultancy, Internet Statistics Compendium 2010 (Feb. 2010), *available at* http://econsultancy.com/ reports/internet-statistics-compendium (reporting that 38% of Gen Y users have an iPhone or iPod touch).

50. *See supra* notes 7-9, and accompanying text.

51. *See, e.g.,* Bus. Software Alliance, *supra* note 1 at 19 (BSA opposes termination of ISP services without due process).

52. *See, e.g.*, Golumbic, *supra* note 34 at 78-79 (citing *Junger v. Daley*, United States Secretary of Commerce 209 F.3d 481 (6th Cir. 2000)) (demonstrating the failure of DRMs by pointing out that a Norwegian teenager was able to write a program that rendered the film industry's investment in a DRM, known as "Contents Scramble System," ineffective).

53. *See* Where's The Beef?, *A Guide to Internet Piracy,* 2006 Hacker Quarterly Summer 2004 , *available at* http://web.archive.org/web/20070512002747/old.wheresthebeef.co.uk/show.php/guide/2600_Guide_to_Internet_Piracy-TYDJ.txt (describing the intricate ranking and distribution employed for piracy).

54. Wired.com, *The Shadow Internet*, http://www.wired.com/wired/archive/13.01/topsite_pr.html; Michael Warnecke, *To Rid Wed of Counterfeit Goods, Rights Holders Turn to Multi-Prong Attack,* 72 Patent, Trademark & Copyright J. (BNA)31 (May 2006) (documenting the failed attempts of police to stop digital piracy).

55. *See* Henry H. Perritt, Jr., *Jurisdiction in Cyberspace in* Borders in Cyberspace: Information policy and the Global Information Infrastructure, 164-202 at 167-78 (Brian Kahin & Charles Nesson eds., MIT Press 1999) (discussing the problems with traditional jurisdiction over digital piracy and suggesting the use of a 'Virtual Arbiter').

the courts must determine which law to apply for cases involving foreign infringement.[56] These decisions take time, money, and manpower that is unnecessary. Considering that infringement of American copyrights is occurring worldwide, any private action against foreign infringers will be severely limited. Customs, on the other hand, will not have jurisdictional problems, as Customs has authority over imports and can apply American law to the digital imports identically to how Customs applies the law to physical imports.

First, if an infringer is foreign, it will be extremely hard for the court to assert jurisdiction. When determining jurisdiction in *Metro-Goldwyn-Mayer Studios Inc. v. Grokster, Ltd.*, the court was only able to establish jurisdiction under the doctrine of specific jurisdiction, asserting that the defendants' distribution of the infringing software was the 'but for' cause of the alleged infringement.[57] This jurisdictional determination has been criticized for establishing attenuated jurisdiction, and the court even recognized that viewing an infringing website's content would typically not give rise to specific jurisdiction.[58] Even if a private agreement between copyright holder and ISPs was finalized, once an infringing use was found, remedy would need to be sought through federal courts, and establishing jurisdiction in each and every case will be a difficult and expensive endeavor. In contrast, Customs should not have any problems establishing jurisdiction as it has enforcement power over imported items.

Second, the adjudicating court must determine which law to apply to the case at hand. The Berne Convention requires national treatment, which requires the court to afford the same protection to foreign copyright holders as they would afford to national authors.[59] Further, article 5.2 of the Berne Convention calls for the adjudicating court to apply the law of the member country where protection is claimed.[60] However, this convention was crafted when copies were created successively, one country at a time, in tangible copies, not when infringement was occurring over the Internet. Internet piracy allows copies to be made in many countries simultaneously, and article 5.2 would require the court to apply the laws of every country in which a copy was made.[61] This is not only difficult, but time consuming, costly and extremely confusing. In contrast, Customs has designated regulations and generally follows the ruling of the American courts when determining if an import is infringing.[62]

Finally, if copyright holding industries and ISPs enter into a private agreement, without government assistance, any enforcement actions taken will be made without affording the infringer due process and will not allow users to defend themselves. Customs currently implements a notice system which affords the infringer an opportunity to fight the decision. Further, Customs decisions are made by impartial lawyers who have experience determining whether a good is infringing. If ISPs were to make unilateral decisions to shut off Internet services based on infringing activity, Internet users could be improperly banned from access. This is especially important considering fair use. The careful balance between copyright owners' rights and fair uses must be respected, and this balance will not be struck if independent determinations of infringement are excluded from ISP service decisions. The law is ever-evolving, especially with regards to copyright in cyberspace, so it is important to have a responsive agency or law making body, such as Customs, involved in infringement determinations in order to properly reflect any changes in the law.

C. Current Efforts

Around the globe there have been some efforts to include ISPs and to begin to monitor Internet activity. On the international level, the Anti-Counterfeiting Trade Agreement ("ACTA") negotiations have been ongoing and are a major source of debate.[63] However,

56. *See generally* Computer Science and Telecommunications Board for the National Research Council, *The Digital Dilemma: Intellectual Property In the Information Age* at 54-61 (analyzing the complexities involved in adjudicating copyright disputes with respect to multiple national laws).

57. 243 F. Supp.2d 1073, 1085 (C.D. Cal 2003) ("[the] second prong of jurisdictional analysis is met if, but for the contacts between the defendant and the forum state, the cause of action would not have arisen").

58. *See id*. *See also* Eliza Shardlow Clark, *Online Music Sharing in a Global Economy: The U.S. Effort to Command (or Survive) The Tidal Wave,* 14 Minn. J. Global Trade 141 (Winter, 2004) at 148 (criticizing the court's exercise of jurisdiction for only conducting a cursory analysis).

59. Berne Convention, *supra* note 24 at 5.1.

60. Berne Convention, *supra* at 5.2 (lex loci protectionis).

61. *See id; See also* Racquel Xalabarder, *Copyright: Choice of Law and Jurisdiction in the Digital Age*. 8 *INT'L COMP. L.* 79 (2002).

62. *See supra*, notes 31-33 and accompanying text.

63. *See e.g.,* Electronic Frontier Found., The Anti-Counterfeiting Trade Agreement, *available at* http://www.eff.org/issues/acta (arguing that ACTA will violate Internet users' rights). The ACTA is such a source of controversy that an entire paper could be devoted to this subject alone, but for the purposes of this paper it is important to note that ACTA negotiations have allegedly covered

this agreement has been negotiated in secrecy, so any speculation as to what ACTA will require is based off of alleged leaks, unconfirmed allegations, or brief fact sheets. Additionally, in Europe, the European Council has issued non-binding directives trying to solve the digital piracy problem. Finally, on a national level, many countries have implemented policies to try to combat digital piracy, most notably France's HODAPI law which attempted to enact a three strike policy.[64]

There are theories that ACTA will require a three-strike rule similar to the HODAPI law in France.[65] However, without government enforcement, any policy adopted in the US will be devoid of due process and thus likely unconstitutional. Further, the United States Trade Representative ("USTR") has stated that one of the goals of ACTA is to "establish enforcement practices that promote strong intellectual property protection in coordination with right holders and trading partners."[66] The USTR further stated that areas for possible provisions include criminal enforcement, border measures, and Internet distribution and information technology, among others.[67] Allowing Customs to take an expanded role in Interment enforcement would address all of these areas while promoting strong intellectual property protection in coordination with rights holders as well as trade partners. Further, ACTA will allegedly include some version of a global DMCA which should include terms that require ISPs to "put in place policies to deter unauthorized storage and transmission of IP infringing content."[68] If these allegations are truly what will be included in the ACTA, then an expanded role for Customs in Internet enforcement will begin to accomplish these goals and will offer a model of enforcement for countries worldwide.

Next, Europe has taken actions which indicate global support for an increased Customs role in monitoring the e-borders. Although there is no such thing as "European copyright law," the European Council has published directives to guide national lawmaking.[69] For example, the Enforcement Directive requires member states to apply effective, dissuasive, proportionate, fair and equitable measures, procedures and remedies against those engaged in counterfeiting and piracy, such as ensuring implementation of access to evidence.[70] Although the E-Commerce Directive prohibits Member States from imposing general obligations to monitor ISPs, it allows Member States to establish obligations where ISPs promptly inform authorities of the identities of recipients of their service with storage agreements.[71] Additionally, the recently approved "Telecoms Package" requires ISPs to comply with the Enforcement Directive.[72] This contradictory language epitomizes the most controversial issue with monitoring the Internet: balancing privacy and freedom of expression against the rights of copyright owners.

While an expanded Customs role in policing digital piracy might conflict with the E-Commerce Directive, it is in line with the newly approved "Telecoms Package." Under the E-Commerce Directive, Customs would essentially be acting as "the authority" to which violating storage service would be reported to. Although it is not essential that a plan allowing Customs to monitor digital imports align with European Directives, a plan that does so will help ACTA negotiations working to improve global enforcement.

ISP cooperation and the enforcement of intellectual property rights over the Internet.

64. *See* Nate Anderson, *France passes harsh anti-P2P three-strikes law*, ArsTechnica.com, *available at* http://arstechnica.com/tech-policy/news/2009/09/france-passes-harsh-anti-p2p-three-strikes-law-again.ars.

65. *See, e.g.,* Michael Geist, *The EU ACTA Consultation: European Commission vs. European Parliament*, *available at* http://www.michaelgeist.ca/content/view/4894/125/ (fearing a three strike policy in ACTA).

66. Office of U.S. Trade Representative, Fact Sheet: Anti-Counterfeiting Trade Agreement (Oct. 2007), *available at* http://www.ustr.gov/sites/default/files/uploads/factsheets/2008/asset_upload_file760_15084.pdf.

67. *See id.* A concern might be that trading partners begin to rely on the United States to enforce intellectual property rights and relax on enforcement efforts within their own borders.

68. Gwen Hinze, *The Anti-Counterfeiting Trade Agreement*, Electronic Frontier Foundation, *available at* http://www.eff.org/deeplinks/2009/11/leaked-acta-internet-provisions-three-strikes-and-.

69. *See* P. Sean Morris, *Pirates of the Internet, at Intellectual Property's End With Torrents and Challenges for Choice of Law* 17 Int'l J. of L. & Info. Tech. (2009) (canvassing the European Directives).

70. Directive 2004/48/EC of the European Parliament and of the Council of 29 April 2004 on the enforcement of intellectual property rights, *Official Journal of the European Union* L 195/16, 2 June, 2004. (aiming to harmonize Member States legislations, so IP owners may enjoy an equivalent level of protection in the European market).

71. Directive 2000/31/EC of the European Parliament and of the Council of 8 June 2000 on certain legal aspects of information society services, in particular electronic commerce, in the Internal Market ('Directive on electronic commerce'), *Official Journal C* 178, 17.07.2000, p.1. at Article 15.

72. Press Release, *Telecoms Package: EU-Wide Spectrum Management for Full Benefits of Wireless Services*, July 7, 2008, (Telecoms Package was adopted, requiring ISPs to comply with the Enforcement Directive).

Regardless of Customs' compliance with European Directives, the contradictory nature of the European Directives highlights the fact that any solution must carefully consider privacy and due process in addition to copyright owners' rights.

Finally, any plan to allow Customs to take an increased role in thwarting digital piracy can be molded around plans that have been invoked on a national level around the globe. First, in France, the Olivennes Agreement was formed between the film industry, music industry, and ISP's devising a gradual punishment approach.[73] This was quickly struck down, but eventually led to a three-strike approach abbreviated in France as HODAPI. HODAPI was also struck down by the courts, in part for failing to afford citizens due process.[74] The court found that any punishment removing Internet access would require judicial adjudication, not administrative proceedings which assume guilt.[75] These rulings may seem fatal to any plan in the United States excluding the judiciary, however, Customs' system for evaluating possible infringement is more than just a determination and allows individuals to submit briefs defending their position.[76] Further, Customs is bound by the law of the courts and enforces the laws of the United States. [77] As such, Customs should be able to work with ISPs to police digital piracy and by doing so Customs will be in line with the goals of ACTA, in harmony with the current European Directives and can avoid the past problems seen on a national level like those seen in France.

IV. Conclusion

Due to the massive amount of piracy occurring throughout the world, action must be taken in some form to protect copyright owners. The Internet is growing at an outstanding rate, and every day billions of users worldwide access the Internet. In the United States, the Internet is a vital aspect of everyday life andrepresents the imminent future of many developing countries. It is time for the United States to finally get ahead of pirates and take enforcement efforts to the Internet while it is still able to do so in a cost-effective and efficient manner. Although Customs will not be able to completely stop digital piracy, it is a start that will give the United States vital experience in dealing with the digital piracy of tomorrow. Involving Customs will avoid the traditional problems seen in federal courts, and seems to be a solution that ACTA and the rest of the world would favor. Pirates will keep coming up with new methods for stealing copyrighted material, so enforcement measures must evolve concurrently. However, the United States cannot wait until pirates reach a plateau; Customs should begin to police digital piracy today.

73. O. DUMONS, «Mission Olivennes: signature de l'accord sur fond de grincements de dents», *Le Monde*, 23 novembre 2007; http:// www.culture.gouv.fr/culture/actualites/index-olivennes231107.htm. (requiring the ISP to send a warning to a client upon detecting infringing activities, and if the user repeats his crime, the user risks having Internet suspended or shut down by the ISP and his name blacklisted).

74. *See* Nate Anderson, *French Court Savages "Three-Strikes" Law, Tosses It Out*, ArsTechnica.com, *available at* http://arstechnica.com/tech-policy/news/2009/06/french-court-savages-3-strikes-law-tosses-it-out.ars (reporting that HODAPI passed on second attempt but was tossed out by the courts).

75. *Id.* ("The Council's censure appears to mean that disconnections—a penalty that the industry says is essential—must be treated like court cases, not "you're probably guilty" administrative proceedings.").

76. *See supra* notes 31-33 and accompanying text.

77. *See supra* notes 28-30 and accompanying text.