American University Law Review

Volume 50 | Issue 2 Article 7

2000

COMMENT: A Nation of Felons?: Napster, the Net Act, and the Criminal Prosecution of File-Sharing

Aaron M. Bailey
American University Washington College of Law

COMMENT: A Nation of Felons?: Napster, the Net Act, and the Criminal Prosecution of File-Sharing

COMMENT

A NATION OF FELONS?: NAPSTER, THE NET ACT, AND THE CRIMINAL PROSECUTION OF FILE-SHARING

AARON M. BAILEY*

TABLE OF CONTENTS

Introduction 474
I. Background 478
A. The Fury Over MP3 "File-sharing" 478
1. Technology 478
2. Why prosecute, and who? 481
a. Potential defendants 482
b. Prosecutors 484
c. Victims 485
B. The Object of "Theft": Copyright as Property, Infringement and Defenses 488
1. What is being "stolen"? 488
2. Criminal infringement before the rise of the internet 489
3. Copyright Felony Act of 1992 and No Electronic Theft Act of 1997 491
4. Contributory and vicarious infringement 493
5. Defenses to criminal infringement 497
a. Substantial noninfringing uses 498
b. Fair use 500
6. Copyright legislation in the digital age 502

* Editor-in-Chief, *American University Law Review*, Volume 51; J.D. Candidate, 2002, *American University, Washington College of Law*; M.A., 1998, *American University*; A.B., 1995, *Wabash College*. The author thanks the many people who made this Comment possible, including Professor Peter Jaszi, Russell Upton, and Antonia Fasanelli. Special thanks go to Susan K. Nutter and my parents, Al and Teresa Bailey, without whose support the entire project would have been impossible.

II. Analysis....506
A. Is File-Sharing an Inherently Criminal Activity? 506
B. Criminal Liability for FTSs? 509
1. Contributory and vicarious criminal liability....509
2. Conspiracy and accomplice liability....511
C. Criminal Infringement and File-Sharing Software Users....513
1. Identification of criminal infringers 514
2. The elimination of the profit motive, the value of infringed works, and fair use 518
3. "Willful" infringement 522
4. Constitutional constraints to enforcement: The Fourth Amendment....524
5. Entrapment 529
6. Jurisdiction 530
Conclusion 531

> Mr. Levy's case should serve as a notice that the Justice Department has made prosecution of Internet piracy one of its priorities . . . . Those who engage in this activity, whether or not for profit, should take heed that we will bring federal resources to bear to prosecute these cases. This is theft, pure and simple.[1]
>
> James K. Robinson,
> Assistant Attorney General

INTRODUCTION

At the beginning of the new millennium, time and space are no longer obstacles to the flow of information and ideas.[2] The Internet revolution is changing the way we live, work, and entertain ourselves.[3]

1. Ashbel S. Green, *Net Piracy Law Gets First Conviction: UO Student*, PORTLAND OREGONIAN, Aug. 21, 1999, at A1 (noting that the prosecution of Jeffrey Levy for criminal infringement of software and other protected works was the first successful prosecution under the No Electronic Theft (NET) Act of 1997).

2. *See* BRYAN ELLICKSON, GAUGING THE INFORMATION REVOLUTION 1-3 (1991); National Research Council, *The Digital Dilemma: Intellectual Property in the Information Age*, *at* http://books.nap.edu/ html/digital_dillemma/exec_summ.html (last visited May 22, 2000).

3. *See* DAN MABRY LACY, FROM GRUNTS TO GIGABYTES: COMMUNICATIONS AND SOCIETY 152-56 (1996) (describing the "explosion" of information technologies in the latter half of the twentieth century, including the advent of the "information highway"); David Beckman & David Hirsch, *We Log On, Therefore We Believe: Philosophically Speaking, the Internet is Creating a New Reality*, 86 A.B.A. J. 74 (2000) (arguing that attorneys must be cognizant of the Internet because it is homogenizing the way people view the world around them and speaking effectively to a jury requires knowledge of this Internet-reality); Peter Magnusson, *The Internet Revolution History and Significance* (Feb. 5, 1997), *at* http://www.sics.se/~psm/ar97/sld003.htm (noting that "[t]he Internet represents a fundamental and extensive force of change that will leave few areas of our lives unaffected"); National Research Council, *The Digital Dilemma: Intellectual Property in the Information Age*, *at* http://books.nap.edu/html/digital_dillemma/exec_summ.html (last visited May 22,

At the same time, the Internet is also changing the way laws are broken.[4]

Internet-related technologies have recently become the focus of criticism and mild paranoia.[5] For many, the focal point of this fear is the increasingly ugly battle centered on the distribution of copyrighted music via the Internet using a digital format known as "MP3."[6] Some critics argue that the monetary survival of artists is at stake because of the e-assault on copyright law led by "file-sharing" companies like Napster.com.[7] Nevertheless, prosecutors have not yet filed criminal charges against these particular, alleged enemies of copyright.[8]

Although lawsuits may put MP3-trading Web sites out of business, the problem of file-trading will not end with Napster and its clones. Napster, which relies on an index available on a central server, is a

---

2000); COMPUTERS AND SOCIETY 2-5 (Colin Beardon & Diane Whitehouse eds., 1993).

4. *See* Laura Ann Forbes, Note, *A More Convenient Crime: Why States Must Regulate Internet-Related Criminal Activity Under the Dormant Commerce Clause*, 20 PACE L. REV. 189, 192 (1999) (noting that the Internet has provided a "new instrumentality" for criminals to commit old-fashioned crimes); Robert L. Ullmann & David L. Ferrera, *Crime on the Internet*, 42 BOSTON B.J. 4, 4 (1998) (noting that Internet crimes have grown in number along with the number of users and that the costs to businesses are astoundingly high).

5. One group of outraged music fans created a web site in an effort to sabotage Napster, explaining that its mission is to create "a monkey wrench in the machinery of online piracy" and noting that "[p]erhaps [this time web anarchy is] taking a form that shakes up your comfortable little online music shop." *See Cuckoo's Egg Project Home Page*, *at* http://www.hand-2-mouth.com/cuckooegg (last visited July 13, 2000).

6. *See* Tatiana Boncompagni, *After Napster: Controversy Over Music Downloads Spurs Hill Lobbying Campaign*, LEGAL TIMES (Washington, D.C.), Aug. 14, 2000, at 1 (noting that both Napster and the RIAA procured the services of lobbyists in Washington in an effort to secure beneficial legislation); Patricia Jacobus, *Napster Suit Tests New Copyright Law*, *at* http://news.cnet.com/news/0-1005-202-1679581.html (Apr. 11, 2000) (noting that the RIAA suit against Napster would be a significant test for application of the Digital Millennium Copyright Act); *Major Recording Labels Sue MP3Board on Copyright* (June 23, 2000), *at* http://legalnews.findlaw.com/ legalnews/ s/20000623/n23147889.html (reporting that BMG Music, Sony Music Entertainment, Inc., and Warner Brothers Records had filed a suit against MP3Board, Inc. for facilitating piracy of copyrighted musical works); Andy Sullivan, *Online-Music Fight Comes to Capitol Hill* (July 11, 2000), *at* http://dailynews.yahoo.com/htx/nm/20000711/wr/tech_napster_dc_14.html (describing hearings before the Senate Judiciary Committee concerning Napster.com, Mp3.com and the state of copyright infringement on the Internet); *TVT Records Joins Stars, Labels Against Napster* (June 7, 2000), *at* http://legalnews.findlaw.com/legalnews/s/20000607/technapster.html (noting that a major independent record label had filed suit against Napster, Inc. for alleged copyright infringement).

7. *See* Adam Cohen et al., *A Crisis of Content—It's Not Just Pop Music; Every Industry that Trades in Intellectual Property—from Publishing to Needlework Patterns—Could Get Napsterized*, TIME, Oct. 2, 2000, at 68 (arguing that rampant file-trading threatens the economic survival of creators of intellectual property generally).

8. Prosecutors have filed criminal charges for copyright infringement, but there are no reported cases of prosecutions involving infringement accomplished by the use of file-sharing technology.

vulnerable target because it is susceptible to a legal attack that can possibly shut down its server, which in turn, shuts down its entire system.[9] However, this weakness does not apply to "peer-to-peer" (P2P) technology because P2P does not require a central server.[10] Therefore, in the peer-to-peer universe, there are no companies to sue in the peer-to-peer universe, only individuals. Yet filing civil lawsuits against millions of individual infringers would prove ineffective at best given logistical considerations and the probability that most infringers are probably judgment-proof.[11]

One potential solution suggested by commentators is utilizing the criminal provisions of the Copyright Act to thwart infringers.[12] The severity of the criminal penalties for copyright infringement, it is argued, may provide an effective deterrent.[13] Prosecuting a select few infringers to set an "example" may discourage other potential infringers.[14] Criminal liability for copyright infringement can be distinguished from civil liability in two ways: (1) a *mens rea* requirement of willfulness; and (2) the requirement that the infringement exceed a minimum value.[15] Neither of these requirements poses a significant hurdle for prosecutors.[16]

The United States has prosecuted only one notable case involving factual circumstances to the Napster file-sharing controversy under the criminal copyright infringement statute.[17] In 1999, Jeffrey Levy, a

---

9. *See* John Borland, *Napster-like Technology Takes Web Search to New Level* (May 31, 2000), *at* http://news.cnet.com/news/0-1005-200-1983259.htm (noting that the "decentralized architecture [of Gnutella] means there is no company [or server] against which to file the kind of copyright-infringement lawsuit now facing Napster, a prospect that has worried record executives.").

10. *Id.*

11. *See* Froma Harrop, *Theft from the Lords of Barbarity*, DENV. POST, June 26, 2000, at B6 (noting that peer-to-peer sharing engenders judgement-proof defendants).

12. *See* Karen Bernstein, *The No Electronic Theft Act: The Music Industry's New Instrument in the Fight Against Internet Piracy*, 7 UCLA ENT. L. REV. 325, 340-41 (2000) (arguing for the use of criminal prosecution under Section 506 of the Copyright Act as a means of deterring infringing activities online).

13. *See* Ronnie Heather Brandes et al., *Intellectual Property Crimes*, 37 AM. CRIM. L. REV. 657, 680 (2000) (noting the penalties that the "basic offense" under Section 506 of the Copyright Act carries are a maximum penalty of five years imprisonment, and any subsequent offense can garner up to ten years imprisonment).

14. In oral argument before the Ninth Circuit Court of Appeals, Senior Judge Beezer raised the question of whether criminal prosecutions under 17 U.S.C. § 506 (1994 & Supp. V 1999) would set an example and function to "educate the public." *See* A & M Records Inc. v. Napster Inc., No. 00-16401 (9th Cir. Oct. 2, 2000) (oral argument).

15. *See* 17 U.S.C. § 506(a) (1994 & Supp. V 1999).

16. *See infra* Part II.C.2-3 (discussing the willful infringement requirement that is necessary to trigger criminal liability for copyright infringement).

17. *See* Karen Eft, *Oregon Student Convicted of Software and Music Piracy* (Aug. 20, 1999), *available at* http://ist.berkeley.edu:5555/ News/Articles99/gen.piracy.html (noting that University of Oregon student Jeffrey Levy was the first person convicted

student at the University of Oregon, pled guilty to criminal copyright infringement for his use of school computers to post software and musical works on the Internet thereby making them available for others to download.[18] The "web-hosting" method utilized by Levy for distributing these works[19] differs technologically from the "file-sharing" methods that are now at issue in *A & M Records v. Napster, Inc.*[20] It is important to note that the differences between file-sharing and web-hosting are *de minimis*, for the purposes of legal liability.[21]

However, identifying individual targets for prosecution will present considerable difficulties.[22] First, determining who is a criminal infringer in cyberspace, or even developing the probable cause necessary to search for infringing material, may be impossible in most cases.[23] Second, even if prosecutors can successfully identify targets, P2P technology, Fourth Amendment search and seizure jurisprudence, and the copyright doctrine of "fair use" may combine to prevent the successful criminal prosecution of most infringers.[24]

This Comment explores potential pitfalls in the criminal prosecution of individual "file-traders" for copyright infringement. Part I of this Comment examines the factual and legal background of

---

under the NET Act, shattering the "dangerous misconception among some netizens that the not-for-profit sharing of copyrighted works is cool, culturally speaking, and affirms the distributors' admirable technical prowess" without risk of sanction).

18. *See UO Student Sentenced for Internet Piracy*, PORTLAND OREGONIAN, Nov. 24, 1999, at D9 [hereinafter *UO Student*] (noting that Levy received two years probation for criminal infringement, but would have served a prison sentence if prosecutors' could have proved the value of distributed works exceeded $10,000); Green, *supra* note 1, at A1 (noting that the works Levy distributed included software, digitally recorded movies, and musical recordings).

19. Levy hosted a Web site, known as a "warez site," which users who downloaded material from the site accessed via the World Wide Web. File-sharing software is not confined to the Web, and utilizes a "peer-to-peer" paradigm that differs from the traditional "client-server" paradigm of the Web. *See* Lee Gomes & Lisa Bransten, *Napster Fuels P2P Uproar* (July 5, 2000), *at* http://www.zdnet.com/zdnn/stories/ news/ 0,4586,2598097,00. html (explaining the decentralized nature of P2P technology).

20. No. C 99-05183 MHP, 2000 WL 573136, at *1 (N.D. Cal. May 12, 2000).

21. Copyright law is generally "technology neutral," making an analysis of the apparatus used for allegedly infringing activity irrelevant in most respects. For example, Section 107 of the Copyright Act, which defines the test for "fair use" of copyrighted material, makes no mention of the method used for copying in its four-pronged balancing test. *See* H.R. REP. NO. 94-1476, at 5 (1976) (noting that the "form, manner, or medium" in which a work is fixed does not determine the subject matter of copyright law).

22. Levy operated from a university system, on his own web site, which was easily traceable. Infringers using P2P do not leave the same obvious trail of evidence, presenting different challenges. *See UO Student*, *supra* note 18, at D9.

23. *See infra* Part II.C.1-4 (citing the technical and constitutional impediments to successful prosecution).

24. *See infra* Part II.C.4-5 (exploring Fourth Amendment constraints and the availability of the entrapment defense).

recent litigation involving file-sharing software, including an explanation of the technologies and a review of the parties involved in current litigation. Part I also explores the evolution of the concept of copyright infringement, including the criminalization of, and defenses to, infringement. Part II argues that, even though file-trading is not an inherently infringing activity, individuals using P2P systems can quickly and easily engage in infringing activity that exceeds the criminal threshold. The unique attributes of P2P technology and the Fourth Amendment, however, may prevent the identification of most criminal infringers. Part III concludes that although content producers may wish to push for more vigorous prosecution of criminal copyright infringement, wide-scale enforcement is impossible given current legal and technological realities.

I. BACKGROUND

A. The Fury Over MP3 "File-sharing"

1. Technology

The theft of intellectual property is not a recent phenomenon.[25] The Internet and other digital technologies are merely new potential threats in the history of copyright infringement.[26] These technologies provide the means to accomplish criminal infringement by allowing copying and distribution of works on a massive scale.[27] Understanding the legal debate requires knowledge of the underlying technology. A brief explanation of the most important components of the "file-sharing" system is therefore necessary.

MP3 is an acronym for Moving Picture Experts Group 1 Audio Layer 3.[28] MP3 refers to both the method for the compression of

25. Even though there were earlier copyright infringement cases, the first significant copyright infringement case was decided in England in 1774. *See* Donaldson v. Beckett, 1 Eng. Rep. 837 (1774) (discussing the origins of the rights granted to copyright holders).

26. *See* Victoria Cundiff, *Stop Cyber Theft: Respecting Intellectual Property Rights on the Internet*, 444 PLI/PAT 93, 95 (1996) (noting that the advent of cyberspace dangerously has led some to believe that the intellectual property regime of real-space does not apply to the Internet); Robert P. Merges, *One Hundred Years of Solicitude: Intellectual Property Law 1900-2000*, 88 CAL. L. REV. 2187, 2191 (2000) (noting that "each new technology has produced cries of alarm over our 'outdated' copyright system").

27. *See* Cundiff, *supra* note 26, at 95.

28. The Moving Picture Experts Group (MPEG) is a subsection of the International Organization for Standardization and the International Electrotechnical Commission (ISO/IEC). This group developed the current

audio data and the resulting digital format.[29] To the human ear, a song recorded in MP3 format sounds as pure and crystalline as a song recorded on a Compact Disc (CD).[30] MP3, quite simply, makes the transfer of CD quality musical content via the Internet possible.[31] Though MP3 does not include an integrated copying protection system, there is at least one external encryption application that claims to make MP3s secure.[32] Although MP3 is in itself something of a revolution, other technologies magnify its impact considerably, particularly "file-sharing" software, which assists in the distribution of digital data.[33]

The Web-based company Napster.com[34] uses this type of software.

---

technical standards for Video CDs, MP3s, DVDs, and Multimedia on the World Wide Web. *See Moving Picture Experts Group Homepage*, *at* http://www.cselt.it/mpeg/ (last visited Aug. 1, 2000) [hereinafter *MPEG Homepage*] (describing the nature and functions of MPEG in the production of "an industry worth several tens of millions of dollars").

29. Files that at one time took hours to download, now take minutes, and, when placed on hard drives, occupy only one megabyte of space per minute of music, rather than hundreds of megabytes. This compression rate compares favorably with compact discs, which require ten megabytes per minute. *See* National Research Council, *The Digital Dilemma: Intellectual Property in the Information Age*, *available at* http://books.nap.edu/html/digital_dillemma/ch2.html (last visited May 22, 2000).

30. *See* Akansha Atroley, *Napster: Music to Most Ears*, COMPUTERS TODAY, Aug. 15, 2000, at 80 (explaining that even though the human hearing ranges from twenty hertz and twenty kilohertz, MP3 technology eliminates all frequencies except those to which the ear is most sensitive, in the area of two to four KHz); *see also* Mike Tanner, *MP3 Music Pirates Avoid Legal Action* (May 23, 1997), *at* http://www.wired.com/news/print/ 0,1294,4069,00.html (noting that MP3 "allows for music files . . . that offer near CD-quality sound").

31. *See* Jonathan Yardley, *The Napster Generation*, WASH. POST, May 8, 2000, at C2 (describing MP3s as "an audio file format 'that has been compressed . . . without any noticeable loss in sound quality . . . in a package small enough that it can be downloaded and/or stored on your PC'").

32. *See* Atroley, *supra* note 30, at 80 (describing the "Digibox" from InterTrust, which utilizes encryption technology to secure MP3s, giving paying consumers a "digital key" to access the encrypted MP3).

33. *See* Recording Indus. Ass'n of Am. v. Diamond Multimedia Sys., Inc., 180 F.3d 1072, 1073-74 (9th Cir. 1999) (noting that the "Internet was of little use for the distribution of music" before the invention of the MP3 compression algorithm); Rob Glaser, *Time to Face the (Digital) Music*, WASH. POST, Aug. 24, 2000, at A25 (noting that file-sharing software like Napster and digital music are "opening doors for distribution models that had never before been seriously considered).

34. The press has vilified Napster as the leader in a vast conspiracy of copyright pirates, while other commentators have touted the company as a trust-busting alternative for artists faced with few choices in marketing and distribution outside the "big record labels." *Compare At Last and At Length: Lars Speaks* (May 26, 2000), *at* http://slashdot.org/ nterviews/00/05/26/1251220.stml (explaining Metallica's position on Napster as a threat to artists' rights in an interview with band member Lars Ulrich), *with Internet Music Debate Moves to Washington* (May 24, 2000), *at* http://www.cnn.com/2000/LAW/05/24/mp3.napster.suit/html (noting that some artists have supported Napster as an alternative form of distribution), *and* Chris Nelson, *Digital Nation: Musicians offer their Two Cents on Napster* (June 7, 2000), *at* http://www.sonicnet.com/news/archive/story.jhtml?id=971727 (citing one musician as saying that recording labels are "in bed together" and "greedy" and that regulation

In Napster's P2P model, users connected to the Napster web site can search the computers of other connected users for certain files.[35] The Napster web site serves as a hub connecting users who wish to trade MP3 files;[36] users log-on to the Napster system, which permits them to locate the Internet addresses of other users, and search for files using a method similar to standard search engines like "Yahoo!"[37] Thus, Napster allows virtual P2P[38] transfers, connecting individual users directly to one another. However, users must first connect to the Napster server in order to find the desired file on the index generated by the server's search of currently connected users' computers.[39] Napster is currently configured to transfer only MP3 files, though it could be upgraded to transfer other files, including image files.[40]

---

was preferable to litigation). *See also* Bob Margolis, *Chuck D Praises Napster at Congressional Hearing* (May 24, 2000), *at* http://www.sonicnet.com/news/archive/story.jhtml?id=873083 (reporting that rapper Chuck D urged support for Napster as an alternative for lesser-known artists and others trying to escape the control of the "big four" record labels—Sony, BMG, Warner Brothers, and A & M Records).

35. *See Napster Copyright Policy*, *at* http://napster.com/dmca.html (last visited May 22, 2000) (explaining that Napster is an "integrated browser and communications system" that allows users to "locate bands and music available in the MP3 music format").

36. *See* Karen Heyman, *Pandora's Box: Napster Unleashes Whole New Net Ballgame*, *at* http://www.laweekly.com/ink/00/19/cyber-heyman.shtml (last visited June 16, 2000) ("[T]he (Napster) software indexes the MP3s you've got on your hard drive, then connects to the Napster server and makes your tracks available to anybody who's hooked up at the time—from your hard drive, not from the Napster server.").

37. *See* Sean Portnoy, *ZDNet Full Review: Napster* (July 7, 2000), *at* http://www.zdnet.com/products/stories/pipreviews/0,8827,258242,00.html (noting that Napster performs a search of a "library" composed of the hard drives of users logged on the system at the time of the search).

38. In peer-to-peer configurations, individual computers are linked together directly through the Internet without the assistance of a central server. *See* Gomes & Bransten, *supra* note 19. The standard Internet configuration is the client-server model, in which individuals (clients) link to others through a server which operates much like a telephone switchboard. *See id.* (explaining P2P technology's decentralized character in contrast to older Internet search mechanisms like Yahoo! and noting that Internet moguls have cited P2P technology's potential as a revolutionary technology); *see also* John G. Spooner, *Intel: The Future is Peer* (Aug. 24, 2000), *at* http://www.zdnet.com/zdnn/stories/news/0,4586,2619470,00.html (noting that computer chip manufacturing giant Intel Corp. has stated that it believes the P2P model "will play a major role in the future of computing"). *But see* Todd Spangler, *The Napster Mirage* (July 24, 2000), *at* http://www.zdnet.com/intweek/stories/news/0,4164,2607261,00.html (noting that no current venture using the P2P model is profitable and noting the lack of central control, as well as security and privacy concerns as potential pitfalls).

39. *See* Heyman, *supra* note 36 (noting that the Napster model is a hybrid of P2P and the traditional client-server paradigm).

40. *See* Greg Miller, *Speed Counts with Napster*, *at* http://live.altavista.com/scripts/editorial.dll?efi=900&ci=1946462 (last visited July 7, 2000) (explaining the comparative advantages and disadvantages of Napster, Gnutella and Imesh, and finding Napster to be more user-friendly, while Gnutella offers true P2P sharing but is slower and requires more technological sophistication of users, but allows the

Napster is but one of a host of file-sharing platforms now in use.[41] Other platforms include Gnutella and Freenet that, unlike Napster, are examples of "true" P2P software.[42] These pure P2P systems do not rely on central servers or a connection to a web site search engine.[43] Gnutella and Freenet are also among those platforms that allow users to transfer files in formats other than MP3, including "JPEG" and "MPEG" images,[44] as well as digital video.[45] This system allows users to transfer text, images, and video, thereby increasing the comparative utility of each system as am information distribution platform.[46] These systems will be discussed in greater detail in the discussion of identifying criminal infringers below.[47]

2. Why prosecute, and who?

The debate over MP3s and file-trading is, at its core, about property rights. Thus far, some legally recognized copyright owners are

---

transfer of other forms of data, including "Midi" and image files).

41. *See id.*; Wade Roush, *Napster, Gnutella, and Freenet: Publishing in the Post-Copyright Universe*, *at* http://www.ebooknet.com/printerVersion.jsp?id=2536 (last visited June 14, 2000) (discussing the impact of Freenet, Napster and Gnutella on copyright law and the marketing strategies of content producers).

42. *See id.*

43. *See* Andy Oram, *Gnutella and Freenet Represent True Technological Innovation*, *at* http://www.oreillynet.com/lpt/a/208 (visited July 18, 2000) (describing the technical aspects of Gnutella and Freenet and their relative superiority to Napster, including Gnutella's flexibility in allowing each site in the network of connected users to "contribute to a distributed search in the most sophisticated way it can" by enabling each site to interpret a search string independently).

44. *See MPEG Homepage*, *supra* note 28 (explaining that MPEG-1 is the standard for Video CD); *Welcome to JPEG*, *at* http://www.jpeg.org/public/jpeghomepage.htm (last visited Sept. 5, 2000) (explaining that JPEG is the acronym for Joint Photographic Experts Group, also a working group of the ISO, which creates standards for the compression of still images).

45. Digital video is familiar to anyone who owns a DVD player. While most DVDs contain video originally shot on standard film and later converted into digital format, filmmakers are beginning to use digital equipment to shoot original footage. *See* Jason Silverman, *Learning to Love Digital Video* (Jan. 20, 2001), *at* http://www.wired.com/news/culture/0,1284,40681,00.html; Mark Armstrong, *Hollywood Versus Video Napsters* (May 30, 2000), *at* http://www.eonline.com/ News/Items/0,1,6553,00.html (noting that the film industry is concerned by the potential threat of Gnutella, Freenet and iMesh.com in aiding video piracy on the Internet); *Studios Sue Website Over Movie, TV Piracy* (June 15, 2000), *at* http://legalnews.findlaw.com/legalnews/s/20000615/leisurempaa.html (reporting that the Motion Picture Association of America had filed a copyright infringement suit against IcraveTV.com for allegedly distributing copyright protected video via the Web).

46. *See* Boncompagni, *supra* note 6, at 1 (noting that Gnutella's capability to transfer multiple file types has drawn the attention of the software industry); Gwendolyn Mariano, *Net Film Firm Taps Gnutella for Video Sales* (June 14, 2000), *at* http://news.cnet.com/news/0-1005-202-2080146.html (reporting that Gnutella already has been selected as the vehicle for an online video venture by SightSound.com in conjunction with a Microsoft copyright protection system despite fears of piracy and litigation).

47. *See infra* Part II.C.1.

attempting to defend this property in the civil arena.[48] The media has painted the current litigation as a simple battle between two diametrically-opposed foes,[49] namely "the music industry" and Napster. Generally, by attempting to shut down Napster and similar companies, the plaintiffs believe that they can prevent the widespread unauthorized dissemination of their works, effectively protecting their property interests.[50]

As noted in the preceding section,[51] the plaintiffs' strategy is not a complete solution to this dilemma. Napster is not the only platform for file-trading.[52] True P2P options like Freenet and Gnutella are not susceptible to suit. Furthermore, suing corporate entities is less effective. Therefore, defending intellectual property requires a more direct approach, such as the prosecution of the individuals who use P2P technology for infringing purposes. As in other criminal cases, a criminal infringement prosecution will involve three parties: defendants, prosecution, and "victims."

a. Potential defendants

Individual downloaders are the most likely targets for prosecution because they are most directly responsible for the allegedly infringing activity. Users are a diverse group.[53] Users of file-trading software

48. *See* A & M Records, Inc. v. Napster, Inc., 2000 WL 573136, at *1 (N.D. Cal. May 12, 2000).

49. *See* Sullivan, *supra* note 6 (describing the MP3 debate as a "fight" between "music-industry heavyweights and Internet moguls"); Fred Vogelstein, *Is it Sharing or Stealing?: Entertainment Moguls May Not Be Able to Stop Napster and Gnutella* (June 12, 2000), *at* http://www.usnews.com/usnews/issue/000612/share.htm (noting that content producers have alleged that Napster and Gnutella creators are "part of a rogue computer network determined to bring down the entertainment industry); Teresa Wiltz, *Man vs. Music Machine*, WASH. POST, June 13, 2000, at C1 (recounting one musician's portrayal of Napster as "salvation" from the "music establishment . . . that has enslaved us");

50. *See* Doug Bedell, *Napster Vows Fight After Ruling*, DALLAS MORNING NEWS, Feb. 13, 2001, at A1 (quoting RIAA attorney Chuck Cooper as saying that the United States Court of Appeals for the 9th Circuit's ruling against Napster means that "it's days as an instrument for electronic shoplifting are over").

51. *See supra* Part I.A.1.

52. *See* Bedell, *supra* note 50, at A1 (noting that competitors, including Gnutella, exist).

53. Students, much maligned as a "criminal class" of copyright bandits, form a minority of users, estimated at only 37%. *See* Brad King, *New School of Thought on Piracy* (June 9, 2000), *at* http://www.wired.com/news/print/0,1294,36875,00.html (noting a survey that showed over 58% of Internet users who downloaded "free" music were over thirty years old); Jonathan Cohen, ed., *Study: Canadian Napster Users Buy CDs* (July 12, 2000), *at* http//www.billboard.com/daily/2000/0712_o5.asp (citing statistics from a Solutions Research Group report that found 39% of Canadian music downloaders were over twenty-five, and an additional 32% were between the ages of eighteen and twenty-four). Several surveys suggest that the majority of American users are in the "over thirty" demographic. *See id.* (noting that over 52% of users were older than thirty); *13 Million Americans Downloading Music for*

have many and varying motives for their activities, from gaining free access to pornography and music,[54] to sharing Genome discoveries.[55]

File-trading services ("FTSs"),[56] including Napster.com, MP3.com, and iMesh.com[57] are also potential targets. The FTSs provide services that, in one form or another, help users to find MP3 files offered by other users for exchange, generally in the hope of turning this service into a profitable enterprise.[58] One service model involves the storage of music, previously purchased by users in CD format, on their web site, which could then be accessed by users via the Internet.[59] FTSs hope to profit from the sale and distribution of music in the MP3

Free (June 9, 2000), *at* http://news.cnet.com/news/0-1005-200-2045621.html (citing a Pew Internet Project survey that found 42% of those downloading music via the Internet without paying were between the ages of thirty and forty-nine).

54. *See Gnutella FAQ Page*, *at* http://gnutella.wego.com/go/wego.pages.page?groupId=116705&view=page&pageId=118401&folderId=118398&panelId=119597&action=view (last visited Aug. 21, 2000) (admitting that a large quantity of "objectionable material," including pornography, is traded using the Gnutella software).

55. *See* Kristen Philipkoski, *Gene Research, Meet Napster* (Apr. 5, 2000), *at* http://www.wired.com/news/technology/0%2C1282%2C35404%2C00.html (noting that one human genome researcher was exploring ways to use Napster-like technology to allow scientists to share their research data).

56. Some of the legal literature on this subject has referred to Napster and its progeny as Internet service providers (ISPs) or online service providers (OSPs). However, to apply these terms in a technical legal sense may be presumptuous. Historically, the term ISP applies to services that provide a connection to the Internet, such as America Online, Inc. (AOL) or Starpower, Inc. One of the pivotal questions in the Napster litigation is whether Napster qualifies as a "service provider" within the meaning of 17 U.S.C. § 512, thus qualifying for safe harbor protection. Section 512(d) indicates that service providers that offer "location tools" are to be afforded safe harbor. *See* 17 U.S.C. § 512(d) (Supp. V 1999). Whether this applies to companies that merely offer a location device, like Yahoo.com, or whether it applies only to companies that offer Internet connections as well as location devices, like AOL, is probably a matter of debate. For purposes of clarity, this Comment shall refer to "file-sharing" services like Napster as file-trading services (FTSs). *See* Jennifer E. Markiewicz, Note, *Seeking Shelter from the MP3 Storm: How Far Does the Digital Millennium Copyright Act Online Service Provider Liability Limitation Reach?*, 7 COMMLAW CONSPECTUS 423, 436 (1999) (opining that the key factor in the ISP definition is "facilitation of access to the Internet").

57. IMesh is an FTS that touts itself as the platform for "sharing the world." IMesh is similar to other FTS's in that it offers an application which enables users to search the hard drives of other iMesh users. *See iMesh.com: Using iMesh*, *at* http//www.imesh.com/using.html (last visited Feb. 21, 2001).

58. *See* Christopher Jones, *Open-Source "Napster" Shut Down* (Mar. 15, 2000), *at* http: // www. wired. com / news / technology / 0%2C1282%2C34978%2C00 . html (describing the way in which Gnutella, Freenet, and Napster allow users to connect to one another on the net, the former without a central server, and also describing America Online's cancellation of the official project for fear of copyright infringement liability).

59. *See* Derek Caney, *MP3.com Settles Copyright Suit with 2 Labels* (June 9, 2000), *available at* http://washingtonpost.com/cgibin/gx.cg. . .me=wpni/print&articleid=A28629-2000Jun9 (describing the MyMP3.com service which allowed subscribers to listen to music via the Internet after having the service provider scan the CD in order to verify that the subscriber owned an authorized copy of the work, and noting that MP3.com had claimed that this service constituted "fair use" as mere space-shifting).

format; this goal puts them squarely in competition with the RIAA.[60] Since they are already open to attack in civil proceedings, and it is uncertain whether there is any potential criminal liability for FTSs,[61] they are less likely to be targeted by prosecutors.

Perhaps the most misunderstood of the players in this drama are the file-sharing software designers who create free file-trading software.[62] The motives of the designers are as diverse as the number of software applications.[63] For example, Gene Kan, one of the developers of Gnutella, stated that the goal of the creators of Gnutella was technological advancement, not profiteering or piracy.[64] Freenet creator Ian Clark proclaimed that the impetus behind its creation was concern for freedom of speech, noting that "Freenet [was] designed to make censorship impossible."[65]

b. Prosecutors

It is likely that the U.S. Department of Justice will, in most instances, file the actual charges and prosecute the cases.[66] Local U.S.

60. *See* Recording Industry Association of America, *RIAA Mission Statement*, *at* http://www.riaa.org/About-Who.cfm (last visited Apr. 10, 2001) [hereinafter *RIAA Mission Statement*] (stating that the RIAA is a trade organization whose "members create, manufacture and/or distribute approximately 90% of all legitimate sound recordings produced and sold in the United States").

61. *See infra* Part II.B.1-2.

62. *See* Richard Stallman, *Why Free Software is Better than Open Source*, *at* http://www.gnu.org/philosophy/free-software-for-freedom.html (last modified Dec. 14, 2000) (describing the open-source movement, which calls for transparency or non-encryption of software codes, and the relationship between "open-source software" and "free software").

63. Ian Clarke has stated that he created Freenet expressly for political purposes, including ending government censorship, while Gnutella has been developed as an alternative to older and slower methods for combing the Web for information. *See* Heidi Chambers, *Interview with Nathan Moinvaziri of Gnutella* (July 8, 2000), *at* http://www.dmusic.com/news/news.php?id=2745 (noting that Gnutella has made file-sharing easier but quoting Gnutella web-master Moinvaziri as saying that protecting anonymity was not an issue for Gnutella developers); Leander Kahney, *Alternative Net Protects Pirates* (Mar. 8, 2000), *at* http://www.wired.com/news/technology/0%2C1282%2C34768%2C00. html (quoting Ian Clarke as stating that his "primary motivation [in creating Freenet] was to make it very difficult to censor information").

64. *See* Kurt Nimmo, *Interview with Gnutella's Gene Kan* (May 14, 2000), *at* http://www.jamz.com/?id=417&action=print (explaining that Gnutella is primarily designed as a tool for "real-time searching" that is an advancement over search engines like Yahoo!).

65. *See* Ian Clarke, *My Views on Censorship and Copyright*, *at* http://freenet.sourceforge.net/index.php?page=philosophy (last visited Apr. 10, 2001) (expressing the view that access to information is necessary for open and democratic societies and questioning the value of copyright law in promoting and rewarding creativity).

66. *See* Janet Reno, *Statement by the Attorney General, Symposium of the Americas: Protecting Intellectual Property in the Digital Age* (Sept. 12, 2000), *available at* http://www.cybercrime.gov/ipsymposium.htm (noting the Justice Department's

Attorneys may try most cases, but the Justice Department, which has also recently added a "Cybercrime" section, may provide additional expertise for prosecution teams.[67]

c. Victims

While criminal prosecutions are generally carried out by agents of the government in the legal system of the United States,[68] victims and groups representing their interests often play an important role in urging prosecutors to take action.[69] The RIAA and its member companies are at the forefront of the litigation of alleged MP3 copyright infringement[70] and are also likely to push for increased prosecution of criminal infringement cases in the future.[71]

The RIAA primarily represents major record labels, such as A & M Records and BMG, Inc., which controls the marketing and distribution of artists' recordings.[72] Filing individual civil suits against

---

strong commitment to prosecuting cases and making sure that "serious IP criminals go to jail for significant prison terms" and that they "get the message, and the message must be clear: There is no safe place to hide.").

67.

> The Computer Crime and Intellectual Property Section ("CCIPS") attorney staff consists of about two dozen lawyers who focus exclusively on the issues raised by computer and intellectual property crime. Section attorneys advise federal prosecutors and law enforcement agents; comment upon and propose legislation; coordinate international efforts to combat computer crime; litigate cases; and train all law enforcement groups.

Computer Crime and Intellectual Property Section of the Criminal Division of the U.S. Department of Justice, *Homepage*, *at* http://www.cybercrime.gov (last modified Apr. 5, 2001).

68. *But see* Terry Carter, *Cops in the Cross Fire*, A.B.A. J., Sept. 2000, at 58 (reporting that a little-used Pennsylvania common law doctrine that allows private citizens to press criminal charges has been utilized recently by civil rights advocates in Philadelphia).

69. *See* Ahmed A. White, *Victims' Rights, Rule of Law, and the Threat to Liberal Jurisprudence*, 87 KY. L.J. 357, 358 (1999) (noting the success of the victims' rights movement in the United States, including the proposed constitutional amendment, and claiming that it "threatens to pervert the critical thrust of rule of law by undermining both its facility to bind the contemporary criminal justice system and its jurisprudence to a minimum of rational norms, possibly shattering the construct's capacity to insure a minimally progressive, liberal legal system.").

70. *See* Recording Indus. Ass'n of Am. v. Diamond Multimedia, Inc., 180 F.3d 1072 (9th Cir. 1999); A & M Records, Inc. v. Napster, Inc., No. C 99-05183 MHP, 2000 WL 573136, at *1 (N.D. Cal. May 12, 2000); UMG Recordings, Inc. v. MP3.com, Inc., No. 00-CIV 472 (JSR), 2000 WL 524808, at *1 (S.D.N.Y. May 4, 2000).

71. The RIAA has a strong record of successfully promoting legislative action for its cause, and there is no reason to believe that these efforts will not be duplicated if criminal prosecution appears to be a realistic means. *See* Lewis Kurlantzick & Jacqueline E. Pennino, *The Audio Home Recording Act of 1992 and the Formation of Copyright Policy*, 45 J. COPYRIGHT SOC'Y U.S.A. 497, 499-500 (1998) (describing the lobbying efforts of the industry and RIAA to form copyright legislation in the face of opposition from the consumer electronics industry).

72. *See RIAA Mission Statement*, *supra* note 60 (stating that the RIAA is a trade group representing members of the "recording industry" who "create, manufacture

millions of file-traders is probably an impractical alternative at best, thus it is in the interest of these corporations to see enough individuals convicted in criminal cases to provide a deterrent to others.[73]

The musicians and other artists whose works are the object of file-trading also have a vital interest in the outcome of the MP3 debate. Most of these artists earn their living from the performance and sale of their works.[74] Despite this common ground, artists, particularly musicians, disagree as to whether file-sharing sites pose a threat to the profitable pursuit of their profession.[75] Although some artists feel file-sharing represents a preferable alternative to the "slavery" of working under the major record labels,[76] others see it as "theft, pure and simple," threatening to destroy the entire music industry and

---

and/or distribute approximately 90% of all legitimate sound recordings produced and sold in the United States").

73. Although civil actions may raise public awareness, the threat of criminal penalties may serve as a much more effective deterrent. *See* Daniel S. Nagin, *Criminal Deterrence Research at the Outset of the Twenty-First Century*, 23 CRIME & JUST. 1, 3 (1998) (arguing that the evidence for the deterrent effect of criminal sanctions "is much firmer than it was fifteen years ago").

74. *See Declaration of Steve Wendell Isaacs* (July 26, 2000), *at* http://www.napster.com/pressroom/legal.html (noting that musicians profit from sales and performance of their music, but decrying the publishing process of the major record labels).

75. *See The Future of Digital Music: Is There an Upside to Downloading?, Hearings on Copyright Issues and Digital Music on the Internet Before the Senate Judiciary Comm.*, 106th Cong. (2000) [hereinafter *Future of Digital Music*] (statement of Lars Ulrich, drummer, Metallica) (opining that "if music is free for downloading, the music industry is not viable" and that Napster and its users are guilty of common theft regardless of the use of new technology to accomplish it). *But see* Derek Caney, *Prince Praises Napster, Rips Industry* (Aug. 9, 2000), *at* http://www.zdnet.com/filters/printerfriendly/0,6061,2613714-2,00.html (quoting music giant Prince, who excoriated the RIAA, exclaiming that "[y]oung people . . . need to be educated about how the record companies have exploited artists and abused their rights for so long and about the fact that online distribution is turning into a new medium which might enable artists to put an end to this exploitation"); Gary Graff, *Napster Controversy Splits Musicians*, PITT. POST-GAZETTE, July 16, 2000, at G5 (citing Limp Bizkit, Cypress Hill, and Green Day as bands showing support for Napster, in contrast to Jimmy Buffett, Nikki Sixx of Motley Crue, and Bret Michaels of Poison as concerned about the impact of MP3 trading); Jon Healey, *Music Industry Facing Challenge*, *at* http://www.mercurycenter.com/cgibin/edtools/printpage/printpage.pl (last visited May 30, 2000) ("A slew of lesser-known bands have released free songs in MP3 format in the hope of building an audience."); Robert Lemos, *Hackers Making Napster "Irrelevant"* (July 16, 2000), *at* http://www.zdnet.com/filters/printerfriendly/0,6061,2604185-2,00.html (stating that platforms like Napster may afford smaller artists greater opportunity to market their music without the need for recognition by the music label monopoly).

76. *See* Neil Strauss, *A Chance to Break the Pop Stranglehold*, N.Y. TIMES, May 9, 1999, at 1AR (describing rock artist Prince's performance with the word "slave" written on his cheek in protest of his treatment by the Warner Brothers record label and subsequent use of the Internet to distribute his music independent of the label).

their livelihoods.[77]

Additionally, a curious assortment of miscellaneous interest groups find that the Napster litigation provides a focal point for their cause.[78] Napster defenders chiefly consist of groups claiming to support technological innovation, a robust First Amendment, and a monopoly-free free market.[79] The opponents[80] of file-trading see it as a pernicious threat to creators, potentially destroying the financial incentives to creativity and thus stifling the "Progress of Science and the useful Arts."[81]

The need to balance between protecting and fostering creative interests, and allowing for the development of new technologies provides a fundamental tension in copyright law.[82] How these

77. *See* Ann Powers, *Rock Star vs. Rock Fan: Who Matters?*, N.Y. TIMES, May 21, 2000, at 39AR (comparing Lars Ulrich's reaction to Napster "piracy" to "a schoolboy tattling on the kids who toilet-papered the gym").

78. Though the exact number of groups having declared their positions on Napster is not known, the variety of groups participating as amici curiae is telling. The Association of American Physicians & Surgeons, the Eagle Forum Education and Legal Defense Fund, the Digital Media Association, the Consumer Electronics Association, and the Computer & Communications Industry Association have filed briefs in support of or neutral to Napster, while content producers have generally shown both formal and informal support for the RIAA. *See Napster Legal Documents*, *at* http://www.napster.com/pressroom/legal.html (last visited Apr. 10, 2001) (listing several amici curiae briefs in support or neutral to Napster and providing access to those briefs).

79. *See* Brief of Amicus Curiae Association of American Physicians & Surgeons, Inc. & Eagle Forum Education and Legal Defense Fund, at 4, A & M Records v. Napster, No. 00-16401, No. 00-16403, 2000 WL 1055915 (9th Cir. July 28, 2000) ("First Amendment rights do not lose their protections simply because someone else's interests are harmed, be it harm to a politician or harm to a profit-maximizing corporation."); Brief of Amicus Curiae Ad Hoc Copyright Coalition, Commercial Internet Exchange, Computer & Communications Industry Assoc., Information Technology Assoc. of Am., NetCoalition.com, United States Internet Industry Assoc., and United States Telecommunications Assoc. at 2-3, A & M Records v. Napster, No. 00-16401, No. 00-16403, 2000 WL 1055915 (9th Cir. July 28, 2000); Brief of Amicus Curiae of Copyright Law Professors in Support of Reversal at 2-3, A & M Records v. Napster, No. 00-16401, No. 00-16403, 2000 WL 1055915 (9th Cir. July 28, 2000) (finding that a blanket ruling against Napster would have the dangerous effect of impeding "the Progress of Science and Useful Arts").

80. *See Music Industry, Music Publishers Respond to Napster, Reaffirming District Court's Infringement Findings*, *at* http://www.riaa.com/PR_Story.cfm?id=320 (last visited Sept. 10, 2000) (noting that among those groups supporting the RIAA as amici curiae are: Motion Picture Association of America (MPAA); Software and Information Industry Association (SIIA); American Film Marketers Association (AFMA); Association of American Publishers (AAP); American Society of Media Photographers; Professional Photographers Association; Graphic Artists Guild; Interactive Digital Software Association (IDSA); American Society of Composers Authors and Publishers (ASCAP); Broadcast Music Incorporated (BMI); Producers Guild of America; Directors Guild of America; Writers Guild of America, West; American Federation of Musicians (AFM); Reed Elsevier; American Federation of Television and Radio Artists (AFTRA); Office of the Commissioner of Baseball; National Basketball Association (NBA); Screen Actors Guild (SAG); and Amsong).

81. U.S. CONST. art. I, § 8, cl. 8.

82. *See* CRAIG JOYCE ET AL., COPYRIGHT LAW 1 (5th ed. 2000) (noting that

interests should be balanced, and whether criminalization of an increasingly common behavior should play a role in the resolution of the file-sharing debate are difficult questions. If copyright defenders eventually turn to the criminal law for solutions, the outcome will largely depend on the regime of intellectual property law that is in constant flux.[83]

B. The Object of "Theft": Copyright as Property, Infringement and Defenses

1. What is being "stolen"?

Although one enraged musician testified to Congress that copyright infringement was "theft," the same as if someone "[w]alk[ed] into a record store, grab[bed] what [they] want[ed] and walk[ed] out,"[84] this characterization is not entirely accurate. Copyrights, unlike other objects of "theft," are not tied to their physical manifestations.[85] Indeed, if they were, file-traders would almost never be liable, in civil or criminal actions, because they do not "take" physical objects when they download MP3s.[86] Conversely, when a person walks out of a store with a CD in his pocket, he is charged with theft, not copyright infringement.[87]

Copyright owners possess, by virtue of their copyright, a "bundle of rights," which is defined by statute.[88] Copyright owner's exclusive

---

"[c]opyright is an exceptionally dynamic body of law" and "is a form of legal adaptation, a response to new technologies in the reproduction and distribution of human expression").

83. *Id.*

84. *The Future of Digital Music*, *supra* note 75 (statement of Lars Ulrich, drummer of Metallica).

85. *See* JOYCE ET AL., *supra* note 82, at 141 (noting that copyright "protection extends not to the material object—e.g., the book, canvas, or cassette—per se, but only to the original expression actually fixed in the object").

86. *See supra* Part I.A.1 (assessing the practice of file sharing).

87. *See* Dowling v. United States, 473 U.S. 207, 216-18 (1985) (distinguishing copyright infringement and theft of "goods, wares [or] merchandise").

88.

> Subject to sections 107 through 12(2), the owner of copyright under this title has the exclusive rights to do and to authorize any of the following: (1) to reproduce the copyrighted work in copies or phonorecords; (2) to prepare derivative works based upon the copyrighted work; (3) to distribute copies or phonorecords of the copyrighted work to the public by sale or other transfer of ownership, or by rental, lease, or lending; (4) in the case of literary, musical, dramatic, and choreographic works, pantomimes, and motion pictures and other audiovisual works, to perform the copyrighted work publicly; (5) in the case of literary, musical, dramatic, and choreographic works, pantomimes, and pictorial, graphic, or sculptural works, including the individual images of a motion picture or other audiovisual work, to display the copyrighted work publicly; and (6) in the case of sound recordings, to perform the copyrighted work publicly by means of a digital audio transmission.

rights include the right of reproduction, distribution, and public performance, including public performance by digital audio transmission.[89] Congress and the courts developed special rules that govern the use, and delineate what constitutes misuse, of this special form of property.[90] When pursuing a criminal case, prosecutors must employ theft's analog in the intellectual property world; copyright infringement.[91]

Infringement can be characterized as the "theft" of one or more of the copyright owner's exclusive rights.[92] Thus, to "steal" an owner's copyright, an infringer need only, without authorization, reproduce or distribute a copyrighted work in any form. Copyright is limited, however, by certain statutory exceptions to this general rule.[93] One of these limitations, "fair use" is discussed in depth below.

2. Criminal infringement before the rise of the internet

Since the inception of statutory copyright protection in the United States, Congress consistently has expanded criminal liability and stiffened penalties for copyright infringement.[94] Prior to 1897, no criminal penalties for copyright infringement existed.[95] In 1897, however, Congress passed a bill that provided for criminal sanctions,[96]

---

17 U.S.C. § 106 (1994 & Supp. V 1999).

89. *See id.*

90. *See* ROBERT P. MERGES ET AL., INTELLECTUAL PROPERTY IN THE NEW TECHNOLOGICAL AGE 324-26 (1997) (noting that the copyright regime governs the copying of original works, the creation of "derivative works" and the distribution, performance and display of works).

91. *See Dowling*, 473 U.S. at 217 (noting that although "copyright does not easily equate with theft, conversion, or fraud," the Copyright Act defines a distinct "term of art to define one who misappropriates a copyright . . . infringe[ment]").

92. *See* 17 U.S.C. § 506(a) (Supp. V 1999) ("Any person who infringes a copyright . . . by the *reproduction or distribution* . . . of 1 or more copies or phonorecords of 1 or more copyrighted works which have a retail value of more than $1,000, shall be punished as provided under section 2319 of title 18.") (emphasis added).

93. The Copyright Act provides a number of limitations to an author's exclusive rights, including "fair use," and a number of compulsory licenses. *See id.* §§ 107-122.

94. *See* Mary Jane Saunders, Note, *Criminal Copyright Infringement and the Copyright Felony Act*, 71 DENV. U. L. REV. 671, 673 (1994) (noting criminal liability for infringement did not exist in the United States prior to 1897).

95.

> The first criminal provision in our copyright laws was a misdemeanor penalty added in 1897 for unlawful performances and representations of copyrighted dramatic and musical compositions. In order to constitute a criminal violation, the defendant's conduct was required to have been 'willful and for profit.' Section 104 of the general copyright revision of 1909 extended this penalty to all types of copyrighted works, again if the conduct was done willfully and for profit.

H.R. REP. NO. 102-997, at 3 (1992), *reprinted in* 1992 U.S.C.C.A.N. 3569, 3571.

96. *See* Act of Jan. 6, 1897, ch. 4, 29 Stat. 481-82.

ending the era of purely civil liability.[97] At the heart of the 1897 Act, and until recently all subsequent criminal infringement statutes, were the dual requirements that the infringement be "for profit" and a *mens rea* equal to "willfulness."[98]

For almost ninety years, these *actus reus* and *mens rea* requirements did not change significantly, though the associated penalties increased drastically.[99] After Congress passed a series of legislation in the 1980s,[100] however, prosecutors could charge first time offenders with a felony for simply infringing "sound recording," a violation which could garner up to two years in prison and a fine of up to $250,000.[101] If a defendant was found to have produced or distributed over 1000 infringing copies, a court could sentence the offender to up to five years in prison.[102]

Section 506 of the Copyright Act of 1976 maintained profit motive as an essential element to criminal infringement.[103] New technologies, especially the Internet, and pressure from content producing industries, including the software industry, moved Congress to eliminate this requirement in the 1990s.[104] The fear that "hackers" might do untold damage "for kicks" pushed criminal copyright infringement in the direction of becoming a strict liability crime.[105]

Currently, section 506 of the Copyright Act differentiates criminal infringement liability from civil liability by either the presence of a profit motive or a retail value of infringed works exceeding $1,000.[106] Section 501 of the Copyright Act defines the basic elements of

97. *Id.* (establishing criminal sanctions for illicit performance or representation of dramatic and musical works).

98. For a general discussion of the history of criminal copyright liability, and the *mens rea* requirement in particular, see Ting Ting Wu, Note, *The New Criminal Copyright Sanctions: A Toothless Tiger?*, 39 IDEA 527 (1999) (arguing the "willfulness" requirement of § 506 will preclude many prosecutions and convictions for criminal infringement).

99. *See* Saunders, *supra* note 94, at 674 (noting that while "[c]riminal offenses under the 1909 Copyright Act were punishable as misdemeanor," by 1982 the 1976 Copyright Act had been amended to include felony provisions, including penalties of up to five years imprisonment and $250,000 in fines).

100. *See* Sentencing Reform Act of 1984, Pub. L. No. 98-473, 98 Stat. 1987 (codified as amended at 18 U.S.C. § 3571 (1994)).

101. *See id.* (citing a "lack of comprehensiveness and consistency" in sentencing and purporting to rationalize sentencing though creation of guidelines).

102. *See id.*

103. *See* 17 U.S.C. § 506 (1994 & Supp. V 1999).

104. *See* Saunders, *supra* note 94, at 678-79 (describing the lobbying efforts of the computer industry and the subsequent introduction of legislation by Senator Orrin Hatch).

105. *See id.*

106. *See* 17 U.S.C. § 506 (1994 & Supp. V 1999).

infringement in both criminal and civil cases.[107] As a result of the relative paucity of criminal infringement cases, courts have interpreted the base offense of infringement mostly in civil cases.[108] Nonetheless, such civil precedent is equally binding in the criminal context.[109]

3. Copyright Felony Act of 1992 and No Electronic Theft Act of 1997

With the advancements in copying technologies in the 1980s and 1990s, especially digital and Internet technologies, Congress further stiffened criminal penalties for infringement regime.[110] The Copyright Felony Act (Felony Act) of 1992[111] amended the criminal sanctions for copyright infringement under 18 U.S.C. § 2319, equalizing penalties regardless of the media used.[112] The Act also increased sentences, allowing for imprisonment of first-time offenders of up to five years for conviction on ten or more infringing copies of copyrighted works, value to exceed $2,500, during a six month period.[113] Second-time offenders can be sentenced to ten years imprisonment.[114] Though the sentencing guidelines recommended under the Felony Act seem to indicate a rather draconian turn in the criminalization of infringement, Congress

---

107. *See id.* § 501(a) ("Anyone who violates any of the exclusive rights of the copyright owner as provided by sections 106 through 12[2] . . . or who imports copies or phonorecords into the United States in violation of section 602, is an infringer of the copyright.").

108. The number of reported criminal infringement cases found in a search of Westlaw or LEXIS can be counted on one hand, but the number of civil copyright infringement cases is in the thousands.

109. The criminal sanctions of section 506 are only applicable when infringement, as defined by the civil provisions of section 501, exists. Thus, cases interpreting the base infringement offense, which is civil in nature, have a direct bearing on criminal proceedings. If a court finds that no *civil* infringement exists, there can be no *criminal* infringement. *See* 17 U.S.C. §§ 501, 506 (1994 & Supp. V 1999).

110. *See* Saunders, *supra* note 94, at 678 (explaining that Congress implemented stiffer criminal penalties in order to combat the alleged loss of billions of dollars in intellectual property by the software industry).

111. Pub. L. No. 102-561, 106 Stat. 4233 (1992) (codified as amended at 18 U.S.C. § 2319 (1994 & Supp. V 1999).

112. *Id.*

113.

> (b) Any person who commits an offense under section 506(a)(1) of title 17 —(1) shall be imprisoned not more than 5 years, or fined in the amount set forth in this title, or both, if the offense consists of the reproduction or distribution, including by electronic means, during any 180-day period, of at least 10 copies or phonorecords, of 1 or more copyrighted works, which have a total retail value of more than $2,500

18 U.S.C. § 2319(b)(1) (1994 & Supp. V 1999).

114. *See id.* § 2319(b)(2) ("Any person who commits an offense under [section 506(a)(1) of title 17] . . . (2) shall be imprisoned not more than 10 years, or fined in the amount set forth in this title, or both, if the offense is a second or subsequent offense under paragraph (1).").

attempted to differentiate between "innocent infringers" and more culpable offenders.[115]

Congress enacted the No Electronic Theft ("NET") Act[116] as a reaction to the U.S. District Court for the District of Massachusetts' decision in *United States v. LaMacchia*.[117] The so-called "*LaMacchia* Loophole" prevented the criminal prosecution of copyright infringement where there was no "commercial motive" on the part of the infringer.[118] The NET Act eliminated the need to prove commercial motive, including felony-level liability,[119] and eviscerated the "lack of market share damage" defense for criminal infringement cases.[120]

The NET Act also redefined "financial gain" as "receipt, or expectation of receipt, of anything of value, including the receipt of other infringing works."[121] Thus, section 506 of the Copyright Act now reads disjunctively, allowing criminal charges in cases of infringement for "financial gain, or reproduction or distribution" of the requisite number of "phonorecords."[122]

The NET Act retained "willfulness" as the *mens rea* element of criminal infringement.[123] Willfulness is defined as "voluntarily and

115. *See* H.R. REP. NO. 102-997, at 6 (1992), *reprinted in* 1992 U.S.C.C.A.N. 3569, 3574; *see also* Saunders, *supra* note 94, at 687-88 (opining that it is well settled that willfulness under the Copyright Felony Act requires a "specific intent" on the part of the defendant and does not include "accidental" violations).

116. Pub. L. No. 105-147, 111 Stat. 2678 (1997) (codified as amended at 17 U.S.C. §§ 101, 506, 507; 18 U.S.C. §§ 2319, 2319A, 2320; 28 U.S.C. § 1498).

117. 871 F. Supp. 535 (D. Mass. 1994); *see also* 143 CONG. REC. E1527-01 (daily ed. July 25, 1997) (statement of Rep. Coble) ("The NET Act constitutes a legislative response to the so-called LaMacchia case.").

118. *See LaMacchia*, 871 F. Supp. at 540 (noting that the Senate sponsor of the Felony Act had intentionally retained the requirement of profit motive for criminal infringement).

119. *See Copyright Piracy, and H.R. 2265, and the No Electronic Theft (NET) Act of 1997: Hearing Before the Subcomm. on Courts and Intellectual Property, House Judiciary Comm.*, 105th Cong. 148 (1997) [hereinafter *NET Act Hearing*] (testimony of Cary H. Sherman, Senior Executive Vice President and General Counsel, Recording Industry Association of America).

120. *See* Lydia Pallas Loren, *Digitization, Commodification, Criminalization: The Evolution of Criminal Copyright Infringement and the Importance of the Willfulness Requirement*, 77 WASH. U. L.Q. 835, 845 (1999) (noting that under the NET Act "if a person made a copy of a licensed program from her computer at work for her home computer so that she could continue to work on a project while caring for an elderly relative" it might be actionable as a felony).

121. 17 U.S.C. § 101 (1994 & Supp. V 1999).

122. The Copyright Act defines "phonorecords" as "material objects in which sounds, other than those accompanying a motion picture or other audiovisual work, are fixed by any method now known or later developed," and is thus applicable to MP3s. *See id.*

123. *See* 143 CONG. REC. H9883-01 (daily ed. Nov. 4, 1997) (statement of Rep. Coble) ("[T]he Subcommittee on Courts and Intellectual Property, during its markup of the NET Act, passed an amendment to ensure that the bill would not modify liability for copyright infringement, including the standard of willfulness for

intentionally violat[ing] a known legal duty,"[124] and the Supreme Court held that the willfulness standard is subjective.[125] Thus, the accused's state of mind or beliefs in a criminal infringement case are usually relevant in determining whether an act was committed willfully.[126]

The legislative history of the NET Act, however, indicates a potentially critical redefinition of willfulness. Lawmakers declared that even though the NET Act requires "more than the mere reproduction or distribution of copyrighted works in establishing willfulness,"[127] "proof of the defendant's state of mind is not required."[128] Thus, Congress explicitly attempted to eliminate subjective "ignorance of the law" as a defense to criminal infringement.[129]

4. Contributory and vicarious infringement

Courts recognize three distinct tiers of liability for infringement,[130]

---

criminal infringement.").

124. *See* United States v. Cheek, 498 U.S. 192, 201 (1991) (citing United States v. Bishop, 412 U.S. 346, 360 (1973)) (noting the defendant's good faith belief that tax laws were unconstitutional need not be found objectively reasonable before being heard by a jury).

125.

> We thus disagree with the Court of Appeals' requirement that a claimed good-faith belief must be objectively reasonable if it is to be considered as possibly negating the Government's evidence purporting to show a defendant's awareness of the legal duty at issue. Knowledge and belief are characteristically questions for the factfinder, in this case the jury. Characterizing a particular belief as not objectively reasonable transforms the inquiry into a legal one and would prevent the jury from considering it. It would of course be proper to exclude evidence having no relevance or probative value with respect to willfulness; but it is not contrary to common sense, let alone impossible, for a defendant to be ignorant of his duty based on an irrational belief that he has no duty, and forbidding the jury to consider evidence that might negate willfulness would raise a serious question under the Sixth Amendment's jury trial provision.

Cheek, 498 U.S. at 203-04.

126. *See* United States v. Moran, 757 F. Supp. 1046, 1051 (D. Neb. 1991) (holding that the beliefs of the defendant in regard to his conduct determines willfulness in a criminal copyright infringement case).

127. 143 CONG. REC. H9883-01, H9884 (daily ed. Nov. 4, 1997) (statement of Rep. Coble).

128. *Id.* (statement of Rep. Coble).

129. The legislative history of the NET Act appears to indicate that criminal infringement is meant to be a strict liability crime. The stipulation that mere evidence of reproduction and distribution is not enough to establish willfulness is part of a larger concern that "third parties," such as ISPs, be exempted from the "volitional" acts of others. *See id.* (statement of Rep. Coble). *But see* Loren, *supra* note 120, at 887-90 (arguing forcefully that the willfulness standard should require that the government "prove an intentional violation of a known legal duty").

130. The Copyright Act is devoid of any mention of theories of secondary liability, which have developed as a matter of common law since the inception of the 1909 Copyright Act. *See* Buck v. Jewell-La Salle Realty Co., 283 U.S. 191, 197 (1931)

depending largely on the degree of participation in the infringing activity. The simplest form of liability, generally involving active participation on the part of the infringer, is direct liability.[131] Direct infringement results from the unauthorized exercise of one or more of a copyright owner's exclusive rights.[132] For example, persons who obtain a work that is subject to copyright protection, copy that work without permission, and transfer those copies to other persons, are liable for "direct" infringement for unauthorized reproduction and distribution.[133] Secondary liability concepts, including vicarious and contributory liability, have been adopted in copyright jurisprudence.[134]

Courts developed a special test for vicarious liability in copyright infringement cases.[135] Both the U.S. Courts of Appeals for the Second and the Ninth Circuits held that, when a defendant has the opportunity to infringe and directly benefits financially from the infringement, the defendant may be found vicariously liable.[136] The defendant's knowledge of the infringing act is irrelevant.[137] The distinguishing element of vicarious liability is the defendant's ability

---

(holding a hotel liable for contributory infringement under the 1909 Act in providing patrons with a radio during the broadcast of infringing performances (citing Charles Scribner's Sons, Inc. v. Straus, 210 U.S. 352, 355 (1908))); Kalem Co. v. Harper Bros., 222 U.S. 55, 62-63 (1911) (finding that secondary liability for copyright infringement was not unconstitutional and that supplying the means for infringement and "invok[ing]" it were grounds for liability "on principles recognized in every part of the law").

131. *See* Playboy Enters., Inc. v. Russ Hardenburgh, Inc., 982 F. Supp. 503, 512 (N.D. Ohio 1997) (noting that direct liability requires that an infringer engage in one of the activities reserved to copyright owners under 17 U.S.C. § 106).

132.

> Anyone who violates any of the exclusive rights of the copyright owner as provided by sections 106 through 121 or of the author as provided in section 106A(a), or who imports copies or phonorecords into the United States in violation of section 602, is an infringer of the copyright or right of the author, as the case may be.

17 U.S.C. § 501(a) (1994 & Supp. V 1999).

133. *Id.*

134. *See* JOYCE ET AL., *supra* note 82, at 783 (noting that the legislative history of section 106 suggests the explicit creation of secondary liability for infringement).

135. *See* Gershwin Publ'g Corp. v. Columbia Artists Mgt., Inc., 443 F.2d 1159, 1162 (2d Cir. 1971) (holding that "even in the absence of an employer-employee relationship one may be vicariously liable if he has the right and ability to supervise the infringing activity and also has a direct financial interest in such activities").

136. *See* Fonovisa, Inc. v. Cherry Auction, Inc., 76 F.3d 259, 265 (9th Cir. 1996) (holding that a flea market operator was liable for vendors' sale of pirated records); Shapiro, Bernstein & Co. v. H.L. Green Co., 316 F.2d 304, 309-10 (2d Cir. 1963) (holding that a retailer was vicariously liable for infringement from its lessee's sale of pirated records because it benefited from the infringement, even though the retailer lacked knowledge of the infringement).

137. *See Shapiro, Bernstein & Co.*, 316 F.2d at 308 (finding that courts have consistently employed strict liability for copyright offenses, refusing to honor lack of knowledge as a defense).

to control or supervise the direct infringer.[138] There is, however, no bright line rule concerning the level of control necessary.[139]

The gravamen of copyright holders' complaints against the FTSs is that they facilitate direct infringement and are liable as contributory infringers.[140] In contrast to vicarious liability, control or supervision is not necessary for a finding of contributory infringement.[141] Providing opportunity and inducing infringement have been the bases for numerous findings of liability.[142] In *Screen Gems v. Mark-Fi Records, Inc.*,[143] the United States District Court for the Southern District of New York denied a motion for summary judgment on behalf of the defendant advertising agency in a contributory infringement case because it deemed the issue of whether the defendant's creation of

138. *See* Pinkham v. Sara Lee Corp., 983 F.2d 824, 834 (8th Cir. 1992) (stating that "the elements of vicarious liability" for infringement are "'(1) [t]he right and ability to supervise the infringing activity; and (2) [a]n obvious and direct financial interest in exploitation of copyrighted materials.'" (quoting RCA/Ariola Int'l, Inc. v. Thomas & Grayston Co., 845 F.2d 773, 781 (8th Cir. 1988))). One court noted that vicarious infringement is based on the "well established" *respondeat superior* precepts of tort liability. *See* Demetriades v. Kaufman, 690 F. Supp. 289, 292 (S.D.N.Y. 1988) (distinguishing between vicarious infringement and contributory infringement).

139. Courts tend to engage in an ad hoc factual determination. *See Fonovisa*, 76 F.3d at 262-63 (finding the operator of a swap meet liable for infringing sales of individual vendors because the operator could control access to the meet area); *Gershwin Publ'g*, 443 F.2d at 1162-63 (reasoning that music artists' manager was liable for infringement because he supervised the concerts at which the artists performed); Dreamland Ball Room, Inc. v. Shapiro, Bernstein & Co., 36 F.2d 354 (7th Cir. 1929) (holding that a dance hall owner was liable for infringing performances on the premises because of the ability to control the venue).

140. *See* A & M Records, Inc. v. Napster, Inc., No. C 99-05183, 2000 WL 573136, at *9 (N.D. Cal. May 12, 2000) (noting that the plaintiffs claimed that "Napster willfully turn[ed] a blind eye to the identity of its users" and ignored users' infringing activity even while aiding it); UMG Recordings, Inc. v. MP3.com, Inc., 92 F. Supp. 2d 349, 351-52 (S.D.N.Y. 2000) (noting that although the plaintiffs charged direct infringement by the defendant, MP3.com's claim that it merely facilitated fair use by its consumers was specious since a "space shift" by individuals was not in itself fair use); *see also* Recording Indus. Ass'n of Am. v. Diamond Multimedia Sys., Inc., 180 F.3d 1072, 1074-75 (9th Cir. 1999) (noting that the piracy allegedly enabled by Diamond's Rio MP3 player concerned the RIAA primarily).

141. *See* Playboy Enters., Inc. v. Russ Hardenburgh, Inc., 982 F. Supp. 503, 514 (N.D. Ohio 1997) (finding that providing opportunity for infringement was enough to hold the operator of an electronic bulletin board system liable for the infringing activities of users, given knowledge that infringing activity was occurring); Columbia Pictures Indus., Inc. v. Aveco, Inc., 800 F.2d 59, 64 (3d Cir. 1986) (holding that charging consumers for using facilities to watch videos it was otherwise licensed to rent constituted contributory infringement of plaintiffs' exclusive right of public performance).

142. *See* Elektra Records Co. v. Gem Elec. Distrib., Inc., 360 F. Supp. 821, 824-25 (E.D.N.Y. 1973) (finding defendant liable for contributory infringement where it had rented "Make-a-Tape" machines on its premises and allowed customers to copy plaintiffs' copyrighted works); *Demetriades*, 690 F. Supp. at 292 (noting that liability for contributory infringement is based on "enterprise liability" concepts, which holds one party liable for another's conduct where the party was aware of the tortious conduct and provided substantial encouragement or assistance).

143. 256 F. Supp. 399 (S.D.N.Y. 1966).

advertisements for records at very low prices should have alerted the defendant that the records were pirated.[144] The U.S. Courts of Appeals for the Ninth Circuit, the U.S. District Court for the Northern District of Ohio, and the U.S. District Court for the Northern District of California extended the doctrine of contributory infringement to Internet services and makers of computer equipment.[145] In one case, the court found an electronic bulletin board service operator liable for allowing the plaintiff's copyrighted pornographic images to be uploaded and distributed by users.[146]

The increasing ubiquity of the Internet has encouraged courts to refine the theory of contributory infringement to fit new technology. In *Religious Technology Center v. Netcom Online Communications Services, Inc.*,[147] the United States District Court for the Northern District of California found that an Internet service provider ("ISP") could not be found liable for infringing material posted on its system if it neither knew nor should have known that the material was infringing.[148] This ruling signaled a trend towards the limitation of contributory infringement liability for ISPs, later codified,[149] and distinguished *Netcom* from previous cases.[150] If prosecutors were to try

144. *See id.* at 404 (opining that if the defendant previously had insisted on receiving proof of rights to recordings, based on the low price of the recordings, defendant could be held liable for contributory infringement based on its constructive or actual knowledge of infringement).

145. *See* Lewis Galoob Toys, Inc. v. Nintendo of Am., Inc., 964 F.2d 965, 971-72 (9th Cir. 1992) (finding that the manufacturer of a computer application that allowed consumers to edit the "display" of the plaintiff's video game products was not liable for contributory infringement because the editing constituted fair use); *Russ Hardenburgh*, 982 F. Supp. at 514-15 (finding operators of an electronic bulletin board system (BBS) on the Internet liable for contributory infringement because users of the BBS uploaded plaintiff's works onto the system and distributed them for download); Sega Enters., Ltd. v. Sabella, No. C 93-04260 CW, 1996 WL 780560, at *7-8 (N.D. Cal. Dec. 18, 1996) (finding a BBS operator liable for contributory infringement where users of the BBS traded in copyright-protected video games and the defendant provided, monitored, and operated the equipment and software used for copying the games).

146. *See Russ Hardenburgh*, 982 F. Supp. at 514 (finding that the defendants "clearly induced, caused, and materially contributed to any infringing activity which took place on their BBS.").

147. 907 F. Supp. 1361, 1373-74 (N.D. Cal. 1995).

148. *Id.* at 1372-73 ("The court does not find workable a theory of infringement that would hold the entire Internet liable for activities that cannot reasonably be deterred.").

149. This trend would culminate in the codification of the Netcom decision in the Digital Millennium Copyright Act. *See* 17 U.S.C. § 1201 *et seq.* (1994 & Supp. V 1999). *See* Mark Robins, *Digital Millennium Copyright Act Defenses for Providers of Online Storage Services and Information Location Tools*, 16 COMPUTER LAW. 11, 16-17 (1999) (discussing the DMCA's limitation of liability for ISPs following Netcom).

150. *Compare Netcom*, 907 F. Supp. at 1361, *and Sega Enters.*, 1996 WL 780560, at *8 (holding that liability for contributory infringement requires that the defendant knows, or should have known, of infringing activity), *with* Playboy Enters., Inc. v. Frena, 839 F. Supp. 1552, 1559 (M.D. Fla. 1993) (finding the operator of an

FTSs on criminal infringement charges they would probably have to overcome the presumption of innocent facilitation established in *Netcom*.

5. Defenses to criminal infringement

The defenses used to negate a civil infringement claim may also defeat a criminal infringement charge. As noted above, criminal infringement requires both the necessary state of mind (willfulness) and that the infringed work(s) exceed a value defined by section 506 of the Copyright Act.[151] Failure to meet these elements is fatal to a criminal infringement action, but so too is the failure to defeat a valid defense to the underlying basic infringement offense.

Two affirmative defenses, developed mostly in civil cases, are of particular importance. First, as with civil infringement, the doctrine of "substantial noninfringing uses"[152] will most likely play a key role in

---

electronic bulletin board liable for contributory infringement despite lack of knowledge of the infringing activity or intent to infringe).

151.

> Criminal Infringement.—Any person who infringes a copyright willfully either—(1) for purposes of commercial advantage or private financial gain, or (2) by the reproduction or distribution, including by electronic means, during any 180-day period, of 1 or more copies or phonorecords of 1 or more copyrighted works, which have a total retail value of more than $1,000, shall be punished as provided under section 2319 of title 18, United States Code. For purposes of this subsection, evidence of reproduction or distribution of a copyrighted work, by itself, shall not be sufficient to establish willful infringement. (b) Forfeiture and Destruction.—When any person is convicted of any violation of subsection (a), the court in its judgment of conviction shall, in addition to the penalty therein prescribed, order the forfeiture and destruction or other disposition of all infringing copies or phonorecords and all implements, devices, or equipment used in the manufacture of such infringing copies or phonorecords. (c) Fraudulent Copyright Notice.—Any person who, with fraudulent intent, places on any article a notice of copyright or words of the same purport that such person knows to be false, or who, with fraudulent intent, publicly distributes or imports for public distribution any article bearing such notice or words that such person knows to be false, shall be fined not more than $2,500. (d) Fraudulent Removal of Copyright Notice.—Any person who, with fraudulent intent, removes or alters any notice of copyright appearing on a copy of a copyrighted work shall be fined not more than $2,500. (e) False Representation.—Any person who knowingly makes a false representation of a material fact in the application for copyright registration provided for by section 409, or in any written statement filed in connection with the application, shall be fined not more than $2,500. (f) Rights of Attribution and Integrity.—Nothing in this section applies to infringement of the rights conferred by section 106A(a).

17 U.S.C. § 506 (1994).

152. *See* Sony Corp. v. Universal City Studios, 464 U.S. 417 (1984) (applying the substantial non-infringing use doctrine for the first time in a copyright case). The doctrine of substantial non-infringing uses is probably best defined as a subcategory of "fair use," but for the purposes of this Comment it shall be treated as a separate category because of its importance to the issues explored herein, and in recognition

determining whether FTSs are liable for the infringing activities of some users. Second, fair use, by contrast, is a defense available primarily to individual users, though it has far-reaching implications for FTSs.

a. Substantial noninfringing uses

In *Sony Corp. of America v. Universal Studios, Inc.*,[153] the U.S. Supreme Court borrowed the concept of "substantial noninfringing use" from patent law to address the application of contributory copyright infringement.[154] In *Sony*, Universal Studios and Walt Disney Productions, both content producers, claimed that Sony was guilty of contributory copyright infringement by marketing and selling the Betamax video tape recorder, which allowed its users to make unauthorized copies of television programs.[155]

The Court held that "the sale of copying equipment, like the sale of other articles of commerce, does not constitute contributory infringement if the product is widely used for legitimate, unobjectionable purposes."[156] Because the recorders could be used for "time-shifting,"[157] they could not be prohibited.[158] This apparent extension of protection against contributory infringement claims was tempered, however, by the Court's insistence that the purveyor of the copying device in question did not encourage unlawful copying.[159] The Court noted that if infringing should become "widespread," adversely impacting the market value of copyrighted works, a different outcome might be warranted.[160]

---

of its distinctive features in copyright jurisprudence. *See* MARSHALL LEAFFER, UNDERSTANDING COPYRIGHT LAW 432-42 (3d ed. 1999).

153. 464 U.S. 417 (1984).

154. *See id.* at 434 (*citing* 35 U.S.C. § 271(b),(c), which impose liability for one who "actively induces infringement of a patent").

155. *See id.* at 435 (explaining the development of liability for contributory infringement).

156. *Id.* at 442 (noting further that a product "*need merely be capable* of substantial noninfringing uses" for the manufacturer to escape liability for contributory infringement) (emphasis added).

157. *See id.* (explaining that "time-shifting" was the practice of taping a program for later viewing and that copyright holders suffered no harm because the resulting use was similar).

158. *Id.*

159. *See id.* at 435-38 (contrasting Sony's lack of contact with customers after the sale of the machines with the sale of an unauthorized film based on a copyrighted work to "motion picture jobbers" in *Kalem Co. v. Harper Bros.*, 222 U.S. 55 (1911)).

160.

> A challenge to a noncommercial use of a copyrighted work requires proof either that the particular use is harmful, or that if it should become widespread, it would adversely affect the potential market for the copyrighted work. Actual present harm need not be shown; such a requirement would leave the copyright holder with no defense against

In *Matthew Bender & Co. v. West Publishing Co.*,[161] the U.S. Court of Appeals for the Second Circuit applied this doctrine in finding that a producer of CD-ROM products was not liable for contributory infringement where it copied the "star pagination" of the West National Reporter System.[162] Importantly, though the defendant was found to have copied West's pagination,[163] which West conceded to be fair use, the court noted no evidence that the defendant encouraged its customers to reproduce the protected "arrangement" of the West reporters.[164] Citing *Sony*, the court held that the CD-ROM products had "substantial, if not overwhelming, noninfringing uses" as research and citation tools.[165]

In at least one case, the maker of a product designed primarily to defeat copyright protection systems, a "black box," found shelter under the theory of substantial noninfringing uses.[166] The defendant's software enabled users to break the anti-copying protections incorporated in the plaintiff's diskettes.[167] The Fifth

> predictable damage. Nor is it necessary to show with certainty that future harm will result. What is necessary is a showing by a preponderance of the evidence that some meaningful likelihood of future harm exists. If the intended use is for commercial gain, that likelihood may be presumed. But if it is for a noncommercial purpose, the likelihood must be demonstrated. In this case, respondents failed to carry their burden with regard to home time-shifting.

Id. at 451.

161. 158 F.3d 693 (2d Cir. 1998).

162. *See id.* at 708.

163. The court distinguished between pagination, the location of information within the reporter, and arrangement, or the order of cases within the reporter. *See id.* at 699-700. The court found that West's "thin" copyright applied only to its arrangement of the cases, because the information contained in them amounted to compilations of facts or public material, and the pagination was merely incidental and not the product of a "creative" endeavor. *See id.* at 698-99 (citing Feist Publ'ns, Inc. v. Rural Tel. Serv. Co., 499 U.S. 340 (1991)).

164. *See id.* at 706. *But see* West Publ'g Co. v. Mead Data Cent., Inc., 799 F.2d 1219, 1229 (8th Cir. 1986) (finding that an online database provider's copying of pagination constituted infringement); Oasis Publ'g Co. v. West Publ'g Co., 924 F. Supp. 918, 931 (D. Minn. 1996) (holding that defendant CD-ROM manufacturer infringed West's copyright protections by copying pagination).

165. *See Matthew Bender*, 158 F.3d at 706-07 (finding that although the "CD-ROM products" in question "might be used incidentally to replicate West's arrangement of cases," they had "substantial, predominant and noninfringing uses as tools for research and citation").

166. *See* Vault Corp. v. Quaid Software, Ltd., 847 F.2d 255, 256 (5th Cir. 1988). Vault, a maker of diskettes that prevented users from copying the software written to the diskette, charged Quaid with contributory infringement. *Id.* Quaid designed software specifically for the purpose of countering the copy prevention technology incorporated on Vault diskettes. *Id.* at 257. Citing *Sony*, the *Vault* court held that Quaid's software, RAMKEY, was "capable of substantial noninfringing uses" because it allowed owners of Vault diskettes to make archival copies pursuant to 17 U.S.C. § 117(2), and exonerated Quaid. *See id.* at 262.

167. *Id.*

Circuit found that defendant's product enabled owners of the diskettes to make archival copies, which it deemed to be a substantial noninfringing use.[168] The doctrine of substantial noninfringing uses is a powerful tool in the defensive arsenal of companies developing new technologies, and may well play a decisive role in the MP3 debate. The implications of this doctrine for criminal prosecutions are discussed below.

b. Fair use

Congress and the courts carved out several exceptions to the exclusive rights of copyright holders, including the right, or affirmative defense, of "fair use."[169] Fair use inquiries involve a balancing test in which four factors are considered:

> (1) the purpose and character of the use, including whether such use is of a commercial nature or is for nonprofit educational purposes; (2) the nature of the copyrighted work; (3) the amount and substantiality of the portion used in relation to the copyrighted work as a whole; and (4) the effect of the use upon the potential market for or value of the copyrighted work.[170]

None of these factors is, by itself, dispositive.[171] A bright line test for fair use is not only elusive, but made impossible by this statute.[172] After weighing these factors, certain activities constitute fair use of copyrighted material, such as reproduction for research purposes and use of quotations.[173]

At the heart of the MP3 debate is the question of whether file-trading is a one-of-a-kind phenomenon, or whether it has something more in common with these examples of fair use. Most MP3 cases involve the reproduction or distribution of "whole" works and the creative "nature" of music is clearly "within the core of the copyright's

168. *Id.*

169. *See* 17 U.S.C. § 107 (1994); *see also* National Research Council, *The Digital Dilemma: Intellectual Property in the Information Age*, *at* http://books.nap.edu/html/digital_dillemma/ch6.html (last visited May 22, 2000) (noting that whether fair use is a right or an affirmative defense is a matter of some debate).

170. *See* 17 U.S.C. § 107 (1994).

171. *See* Harper & Row Publishers v. Nation Enters., 471 U.S. 539, 560 (1985) (stating that the four factors are not considered exclusive, but merely the most relevant).

172. *See id.* (noting that fair use "is an equitable rule of reason, [and] no generally applicable definition is possible" (citing H.R. REP. NO. 94-1476, at 65 (1976), *reprinted in* 1976 U.S.C.C.A.N. 5659, 5679)).

173. *See* H.R. REP. NO. 94-1476, at 65 (1976), *reprinted in* 1976 U.S.C.C.A.N. 5659, 5678-79 (citing "quotation of short passages in a scholarly or technical work . . . parody . . . reproduction by a library of a portion of a work to replace part of a damaged copy . . ." as acceptable examples of fair use).

protective" shield.[174] The character of file-trading is, however, not obviously within the prohibited sphere of uses, nor is it certain what effect file-trading has upon the potential market for MP3s.[175]

Courts interpret the "purpose and character" language of section 107 to prohibit uses that are "commercial" in nature,[176] directly benefiting the copier by eliminating the need to purchase the work.[177] Looking to the "nonprofit educational purposes" language of the statute,[178] courts first ask whether a use is "private" in nature, when determining whether the character of the use is non-commercial[179] and, second, whether a use is "transformative."[180] If a use alters a work in a fashion that is either creative or has independent intellectual value it is more likely to be found within the ambit of the fair use doctrine.[181]

The effect of a specific use upon the potential market for a work is often characterized as "the single most important element of fair use."[182] Courts note that the effect on the potential market for the "particular [form of the] work" is the correct focus of the inquiry.[183]

---

174. *See* Campbell v. Acuff-Rose Music, Inc., 510 U.S. 569, 586 (1994) (finding that the musical works of Roy Orbison were among the types of expression afforded the greatest protection by copyright).

175. *See* A & M Records v. Napster, Inc., No. 00-16401, slip op. at 19 (9th Cir. Feb. 12, 2001) (noting that conflicting reports existed as to the damage caused to the CD market, but finding that Napster was detrimental to the plaintiffs' exploitation of the online market).

176. *See* Am. Geophysical Union v. Texaco, Inc., 60 F.3d 913, 922 (2d Cir. 1994) ("The greater the private economic rewards reaped by the secondary user (to the exclusion of broader public benefits), the more likely the first factor will favor the copyright holder and the less likely the use will be considered fair.").

177. *See Harper & Row*, 471 U.S. at 562 (noting that central to the commercial use inquiry is "whether the user stands to profit from exploitation of the copyrighted material without paying the customary price").

178. *See* 17 U.S.C. § 107(1) (1994).

179. *See American Geophysical Union*, 60 F.3d at 922 (finding that fair use is often found where a use "produces a value that benefits the broader public interest (citing *inter alia* Twin Peaks Prods., Inc. v. Publ'ns Int'l, Ltd., 996 F.2d 1366, 1375 (1993); Rosemont Enters., Inc. v. Random House, Inc., 366 F.2d 303, 307-09 (2d Cir. 1966))).

180. *See Campbell*, 510 U.S. at 579 (holding that "[a]lthough such transformative use is not absolutely necessary for a finding of fair use . . . the goal of copyright, to promote science and the arts, is generally furthered by the creation of transformative works" (citing Sony Corp. of Am. v. Universal City Studios, Inc., 464 U.S. 417, 455 n.40 (1984))).

181. *See American Geophysical Union*, 60 F.3d at 923 (noting that non-transformative uses usually present weak arguments for a finding of fair use).

182. *See Harper & Row*, 471 U.S. at 566 (considering the question of whether the unauthorized publication of material from a manuscript constituted fair use and finding that the intent of the defendant to "scoop" the plaintiff in a market precluded a finding of fair use). *But see American Geophysical Union*, 60 F.3d at 926 (claiming that the Supreme Court abandoned this interpretation in *Campbell*).

183. *See American Geophysical Union*, 60 F.3d at 927 (finding that the potential market value of the "individual journal articles" that were copied were the relevant

In addition, the phrase "potential market" includes markets not only currently developed by copyright owners, but also those that are viable for development.[184]

Though each of the defenses discussed above has been developed in the context of the civil law, each has equally important ramifications in the criminal context. The effect of proving fair use or some other valid defense is to negate any claim of infringement, and without infringement there is no civil or criminal liability.[185] As discussed below, the essential line between civil and criminal liability is marked by a difference in motive and volume of infringing activity.[186]

6. Copyright legislation in the digital age

In the 1990s, Congress passed a number of amendments to the Copyright Act in an effort to address new technological challenges. The Audio Home Recording Act (AHRA) of 1992[187] addressed concerns about the copying capacity of digital audio tape (DAT),[188] and the Digital Millennium Copyright Act (DMCA)[189] amended U.S. copyright law in order to comply with the World Intellectual Property Organization (WIPO) treaties,[190] as well as to speak to the challenges of digital technology.[191] One of the significant features of the DMCA

---

scope of inquiry rather than the value or market for "journal issues and volumes").

184. *See id.* at 928-30 (noting that not every conceivable use is a "potential market" use and that courts have limited analysis to "traditional, reasonable, or likely to be developed markets" (citing *Harper & Row*, 471 U.S. at 568; *Campbell*, 510 U.S. at 591-92)).

185. *See* United States v. LaMacchia, 871 F. Supp. 535, 539 (D. Mass. 1994) (noting that the essential difference between criminal and civil liability for copyright infringement from 1897 to 1994 was the "commercial exploitation" of the work by the infringer).

186. *See id.*; 17 U.S.C. § 506 (1994 & Supp. V 1999).

187. *See* Pub. L. No. 102-563, 106 Stat. 4237 (1992) (codified as amended at 17 U.S.C. § 1001 *et seq.*).

188. The AHRA, however, was primarily designed to combat the threats posed by non-cyberspace technologies like DAT; its application to the problem of FTSs offering access to MP3 files may be of somewhat dubious value. *See* Stephanie L. Brauner, *High-Tech Boxing Match: A Discussion of Copyright Theory Underlying the Heated Battle Between the RIAA and MP3ers*, 4 VA. J.L. & TECH. 5, 8 (1999) (discussing the application of fair use doctrine and the AHRA in the Diamond Multimedia Rio litigation).

189. *See* Pub. L. No. 105-304, 112 Stat. 2860 (1998) (codified at 17 U.S.C. § 512 (Supp. V 1999)).

190. H.R. REP. NO. 105-551, pt. 2, at 32-33 (1998) (stating that the committee was balancing the need to honor the United States' commitment to the two WIPO treaties with Congress' commitment to the concept of "fair use").

191. Even though the DMCA purports to clarify the rights and liabilities of ISPs under 17 U.S.C. § 512, it has been a matter of some debate as to whether the rights of content consumers and distributors have been adequately balanced. *See* David Nimmer, *A Riff on Fair Use in the Digital Millennium Copyright Act*, 148 U. PA. L. REV. 673, 675 (2000) (criticizing the DMCA for failing to protect the fair use rights of

is the codification of the *Netcom* ruling's requirement of knowledge or "volition" for contributory liability.[192] ISPs that do not have knowledge of infringing activity cannot be found liable for contributory infringement.[193] These laws are illustrative of the recent trend in Congress towards technology-specific remedies to perceived threats to the current copyright regime.[194] Neither the AHRA or the

---

content users); Damien Cave, *Does Anybody Care About Fighting the DMCA?* (May 19, 2000), *at* http://www.salon.com/tech/log/2000/05/19/dmca/print.html (quoting the director of the American Library Association Office for Information Technology Policy as stating, "[c]ourt cases are cropping up like mushrooms because the law is so vague"); *see also* UCLA Online Institute for Cyberspace Law and Policy, *The Digital Millennium Copyright Act*, *at* http://www.gseis.ucla.edu/iclp/dmca1.html (last modified Feb. 8, 2001) (explaining the background of the DMCA). *But see* Matthew Kane, *Copyright and the Internet: The Balance Between Protection and Encouragement*, 22 T. JEFFERSON L. REV. 183, 199-200 (2000) (arguing the current legal regime adequately balances the interests of users and copyright holders).

192. *See* Markiewicz, *supra* note 56, at 434 (noting section 512 essentially codifies the *Netcom* ruling).

193.

> (a) Transitory Digital Network Communications.—A service provider shall not be liable for monetary relief, or, except as provided in subsection (j), for injunctive or other equitable relief, for infringement of copyright by reason of the provider's transmitting, routing, or providing connections for, material through a system or network controlled or operated by or for the service provider, or by reason of the intermediate and transient storage of that material in the course of such transmitting, routing, or providing connections, if—(1) the transmission of the material was initiated by or at the direction of a person other than the service provider; (2) the transmission, routing, provision of connections, or storage is carried out through an automatic technical process without selection of the material by the service provider; (3) the service provider does not select the recipients of the material except as an automatic response to the request of another person; (4) no copy of the material made by the service provider in the course of such intermediate or transient storage is maintained on the system or network in a manner ordinarily accessible to anyone other than anticipated recipients, and no such copy is maintained on the system or network in a manner ordinarily accessible to such anticipated recipients for a longer period than is reasonably necessary for the transmission, routing, or provision of connections; and
>
> (5) the material is transmitted through the system or network without modification of its content . . . (d) Information Location Tools.—A service provider shall not be liable for monetary relief, or, except as provided in subsection (j), for injunctive or other equitable relief, for infringement of copyright by reason of the provider referring or linking users to an online location containing infringing material or infringing activity, by using information location tools, including a directory, index, reference, pointer, or hypertext link, if the service provider—(1)(A) does not have actual knowledge that the material or activity is infringing; (B) in the absence of such actual knowledge, is not aware of facts or
>
> circumstances from which infringing activity is apparent.

17 U.S.C. § 512(a), (d)(1)(A)-(B) (Supp. V 1999).

194. For example, sections 1002, 1004 of the AHRA also require the compensation of artists and incorporation of "copying controls" by the manufacturers and distributors of digital audio recording devices. *See* 17 U.S.C. §§ 1002, 1004 (1994 & Supp. V 1999). The AHRA clearly envisioned manufacturers of copying hardware directly compensating copyright holders through payment of a

DMCA, however, specifically address criminal copyright infringement.

Though arguably limited to copiers using DAT, language in the legislative history of the AHRA shows some support for the contention that non-commercial copying should be considered fair use.[195] Counsel for Napster attempted to make the AHRA an issue at trial, claiming that its users are engaged in activity protected by the AHRA and hence, Napster cannot be found liable of contributory infringement where there is no direct infringement.[196] Whether the language of the AHRA is sweeping enough to possibly include file-sharing software remains an open question.[197]

---

percentage on each unit sold as well as voluntary installation of copying controls. *See id.* However, most file-trading services neither sell their software (eliminating the need to pay royalties), nor utilize copying controls. *See* Ben Charny, *Glaser: Let's Make Music Napster-Easy* (July 25, 2000), *at* http://www.zdnet.com/zdnn/stories/news/04586,2607181,00.html (reporting Emusic.com offers a library of 125,000 songs for a ten dollar monthly fee); Anne L. DiPasquale, *Copyright Issues of Online Music*, INTERNET NEWSLETTER: LEGAL AND BUS. ASPECTS, Apr. 1999, at 7 (noting the GoodNoise Corporation was recently granted a license to publish music from certain recording companies for 7.1 cents per downloaded song).

195. The legislative history includes one pronouncement that AHRA contains "exemptions from liability for suit under title 17 for home taping of copyrighted musical works and sound recordings . . . . In the case of home taping, the exemption protects all noncommercial copying by consumers of digital and analog musical recordings." *See* H.R. REP. NO. 102-873, pt. 1, at 24 (1992), *reprinted in* 1992 U.S.C.C.A.N. 3578, 3594.

196.

> No action may be brought under this title alleging infringement of copyright based on the manufacture, importation, or distribution of a digital audio recording device, a digital audio recording medium, an analog recording device, or an analog recording medium, or based on the noncommercial use by a consumer of such a device or medium for making digital musical recordings or analog musical recordings.

17 U.S.C. § 1008 (1994 & Supp. V 1999).

The AHRA creates an exemption for certain personal digital copies. *See id.* (creating an exemption for certain personal, digital copies). *See also Copyrights: Ninth Circuit Stays Injunction in Napster Case Pending Appeal*, PAT., TRADEMARK & COPYRIGHT L. DAILY, Aug. 1, 2000, at D2 (noting that the U.S. Court of Appeals for the Ninth Circuit overturned a preliminary injunction, citing unresolved issues including, inter alia, Napster's AHRA defense).

197. "[N]oncommercial" recordings of consumers who use "digital audio recording devices" are exempt from claims of infringement. *See* 17 U.S.C. § 1008 (1994 & Supp. V 1999). Although a file-sharing application like Napster is clearly digital and audio in nature, it is perhaps less certain whether what it does is *recording* and whether it is a *device* within the meaning of the statute. *See id.* Section 1001 defines a "'digital audio recording device'" as "any machine or device of a type commonly distributed to individuals for use by individuals, whether or not included with or as part of some other machine or device," which is primarily designed to make copies "for private use." DAT is clearly the target of the statute. *See id.* § 1001; *see also* H.R. REP. NO. 102-1100, at H783-61 (1992) ("[T]he purpose of the act is to create the necessary legal environment for digital audio technology (DAT) to be commercialized in the United States."); Sheldon W. Halpern, *Copyright Law in the Digital Age: Malum in Se and Malum Prohibitum*, 4 MARQ. INTELL. PROP. L. REV. 1, 8 (2000) (discussing the problems with congress' enactment of the AHRA).

One aspect of the DMCA that may gain importance in the near future is its ban of the circumvention of technological protection measures.[198] As some critics note,[199] 17 U.S.C. § 1201 purports to clarify the prohibition against black box technology, but it also prevents purchasers of copyrighted works from making traditional "fair use"[200] copies of those works.[201] Currently, most musical works, recorded in standard formats like the compact disc, are not protected by such anti-copying technologies.[202] Section 1201 may play a more pivotal role in criminal infringement litigation as protection technology is applied to all musical formats.[203]

Even though fair use provides a defense for individuals, the DMCA's "safe harbor"[204] represents the creation of a special defense for organizations (ISPs) against charges of contributory or vicarious copyright infringement.[205] Section 512 differentiates among several functions, requiring differing methods of compliance[206] for an ISP

198. *See* Pamela Samuelson, *Intellectual Property and the Digital Economy: Why the Anti-Circumvention Regulations Need to be Revised*, 14 BERKELEY TECH. L.J. 519, 537-46 (1999) (averring that the anti-circumvention exceptions are unduly narrow and that circumvention for a number of "legitimate reasons should be privileged").

199. *See generally* Nimmer, *supra* note 191, at 673 (lamenting section 1201's evisceration of fair use rights and possible inauguration of a "pay-per-use" intellectual property regime); Samuelson, *supra* note 198, at 519 (criticizing section 1201 as inhibiting fair use).

200. *See* Nimmer, *supra* note 191, at 723-25 (noting that, though the legislative history of the DMCA purported to make no changes to the fair use doctrine of section 107, section 1201 violations preclude a fair use defense entirely).

201. *See infra* Part I.B.5.b (explaining the fair use doctrine).

202. *See* Jeff Howe, *Net Loss: Music Industry Report Projects Huge Losses to Web Piracy* (May 24-30, 2000), *at* http://www.villagevoice.com/ issues/0021/howe.shtml ("[E]very CD sold in the stores is a CD that someone will post for free online.").

203. Most musical formats do not offer technological protection, such as encryption. This is especially true of the most popular format, the compact disc (CD). Though it is possible to encrypt CDs, the fact that almost all music recorded to date is currently available in unprotected digital format means that this music will remain forever available for pirates to copy without having to bother taking sophisticated, or even basic anti-circumvention measures. *See* Richard Barry, *ECTS: Copying CDs Just Got Harder* (Sept. 7, 1998), *at* http://www.zdnet.co.uk/news/1998/35/ns-5422.html (describing a California-based company's "SafeDisc" software that encrypts CDs with a digital signature). One could foresee a technology that serves both as a distribution device, like Gnutella, and as an circumvention device. Presently, however, such technology remains hypothetical, largely because there is no need for it. *See* Brad Biddle, *Consumer Rights vs. Encryption* (Feb. 23, 1999), *at* http://www.mp3.com/news/178.html (discussing software programs "Total Recorder" and "Audiojacker" and their use as circumvention devices in conjunction with MP3 use and file-trading on the MP3.com site).

204. *See* 17 U.S.C. § 512 (1994 & Supp. V 1999).

205. *See* H.R. REP. NO. 105-551, pt. 2, at 77-84 (1998) (stating that Section 512 provides exemptions for "service providers" defined generally by provision of access to the Internet).

206. *See* 17 U.S.C. § 512(n) (Supp. V 1999) (providing that whether a service provider is held liable under one subsection has no bearing on whether the provider is liable under a separate subsection).

depending on which of these functions it performs.[207] Since the safe harbor provisions are applicable only to service providers that lack the kind of direct involvement and knowledge of questionable file-sharing that FTSs have, section 512 will most likely play a role in civil trials, rather than in criminal prosecutions.

II. ANALYSIS

A. Is File-Sharing an Inherently Criminal Activity?

File-sharing is arguably not intrinsically infringing. Theoretically, there are many non-infringing uses for file-sharing technology. Sharing non-copyrighted works, or works considered to be within the public domain, is not infringement.[208] Thus, using file-sharing software to share public-domain material is one potential non-infringing use.

Similarly, there are some circumstances in which file-sharing may constitute fair use. If, for example, a file containing a "quotation of short passages in a scholarly or technical work"[209] were transmitted via Gnutella for research purposes, the act of transmission would not constitute infringement.[210] Fair use is a technologically neutral

---

207. Section 512, subsections (a) through (d), divides ISP functions into four basic categories; transmission, temporary storage, storage of information on an ISP's system "at the direction of users," and "linking users to an online location containing infringing material or infringing activity." The DMCA requires that, in certain circumstances, parties engaging in one or more of these activities take measures against copyright infringement in order to receive exemption from liability. *See* Irina Y. Dmitrieva, Note, *I Know It When I See It: Should Internet Providers Recognize Copyright Violation When They See It?*, 16 SANTA CLARA COMPUTER & HIGH TECH. L.J. 233, 240-42 (2000) (describing the affirmative defenses created by section 512 and differentiating between the functions performed by ISPs). For instance, some ISPs must take measures to disable access to users or sites that engage in infringing activity. *See* 17 U.S.C. § 512(d)(3) (Supp. V 1999). *But see id.* § 512(d)(1)(A)-(B) (an ISP which functions as a "location tool" is not required to take measures unless it has "actual knowledge" of infringement or is "aware of facts or circumstances from which infringing activity is apparent."). One may contrast section 512(a), applicable to "transitory digital network communications," which does not contain either the "actual knowledge" or the "take down" requirements of section 512(d), which applies to location tools.

208. Generally, copyrights are extinguished seventy years after the death of the author or creator of the work, thus entering the public domain pursuant to 17 U.S.C. § 302(a). Sound recordings are peculiar, however, in that section 301(c) allows state or common law copyright protection of works created prior to 1972, until February 15, 2047. Only as of February 15, 1972, did sound recordings become subject to federal copyright protection. *See* Act of Oct. 15, 1971, Pub. L. No. 92-140, 85 Stat 391.

209. *See* H.R. REP. NO. 94-1476, at 65 (1976), *reprinted in* 1976 U.S.C.C.A.N. 5659, 5678.

210. *See* 17 U.S.C. § 107 (1994) ("[R]eproduction in copies or phonorecords . . . for purposes such as . . . scholarship, or research, is not an infringement of copyright.").

concept, and thus, whether the medium used is a mimeograph or an MP3, fair use copies are not infringing.[211] When file-sharing is non-commercial and does not harm the potential market for the work or data that is traded, there is a strong argument that this activity constitutes fair use.[212]

There are, on the other hand, many potentially infringing uses for file-sharing software. Placing a large quantity of files of proprietary software and musical works on the web for others to download free of charge, constitutes infringement.[213] The file-sharing activities on Napster are arguably similar. Users basically allow their hard drive, or a portion of it, to be searched by other users.[214] In this way, the Napster user's hard drive is essentially made accessible via the Internet, which has the same effect as providing access to infringing material on a web site.[215] Users are "distributing" protected material.[216] Section 106 does not differentiate between the manner in which material is reproduced or distributed,[217] making a distinction based on the difference between "posting" and "trading" meaningless. Fair use is probably not a viable defense when MP3s are

211. The statutory guidelines for fair use do not account for particular methods used for reproduction, focusing instead on the purpose of reproduction and the effect of reproduction on the market for the work. *See* H.R. REP. NO. 94-1476, at 65-66; 17 U.S.C. § 107 (1994).

212. *See* Am. Geophysical Union v. Texaco, Inc., 60 F.3d 913, 922-30 (2d Cir. 1995) (discussing the provisions of section 107 of the Copyright Act and noting that there is a strong presumption that non-commercial uses that have little effect on the market for the work are fair uses).

213. *See* United States v. LaMacchia, 871 F. Supp. 535, 545 (D. Mass. 1994) (suggesting that the prosecution should have charged an MIT student with contributory criminal copyright infringement for facilitating the copying of software and music from his web site).

214. *See* John Borland, *Gnutella Viruses Weaker than Email Bugs, Experts Say* (June 5, 2000), *at* http://www.cnet.com/news/0-1005-202-2020899.html (explaining that the security issues of file-sharing are acute because users "open their hard drives directly to one another, without any way of verifying other peoples' identities or intentions"); *Gnutella Network Frequently Asked Questions*, *at* http://gnutella.wego.com/go/weg.pages.pa. . .olderID=118398&panelId=119597&action=view (last modified May 28, 2000) ("Gnutella only shares the folders which you specify - this can be changed in the configuration area of Gnutella.").

215. *See LaMacchia*, 871 F. Supp. at 536 (describing LaMacchia's posting of software to a BBS, colloquially known as a "warez" cite, for downloading).

216. *See* Linton Weeks, *Don't Steal This Book*, WASH. POST, Aug. 9, 2000, at C1 (noting that the American Association of Publishers has shown concern for the potential threat of illicit distribution and "duplication facilitators like Napster and Gnutella").

217. Fixation (reproduction) is defined by section 101 as fixing a work in an "embodiment . . . sufficiently permanent or stable to permit it to be perceived, reproduced, or otherwise communicated for a period of more than transitory duration." 17 U.S.C. § 101 (1994); *see also* H.R. REP. NO. 94-1476, at 62 (1976), *reprinted in* 1976 U.S.C.C.A.N. 5659, 5675 (noting that the unauthorized "first public distribution of an authorized copy" as well as "unauthorized public distribution of copies or phonorecords that were unlawfully made would be an infringement").

traded. The downloader does benefit directly, "profit[ing] from the exploitation of the copyrighted material without paying the customary price."[218] Also, a defendant need not make a business of infringement, so long as they get for free something for which they otherwise would have had to pay.[219]

Though it is less certain whether the potential market for musical works, in general, is harmed by MP3 trading,[220] courts interpret section 107 to require that a use not compete with "traditional, reasonable, or likely to be developed markets" in order to be afforded protection.[221] Because the record labels are already pursuing sales of MP3s or their equivalent online,[222] a court could easily find that file-trading negatively impacts the market for music sales *online*.[223] Assuming that at least some of the activity on FTSs is infringing, it is possible that individual users and/or the FTSs may be subject to charges of criminal infringement.

---

218. *See* Harper & Row Publishers v. Nation Enters., 471 U.S. 539, 562 (1985) (noting that central to the commercial use inquiry is whether the defendant gains from not having to pay for a work otherwise unavailable).

219. *Id.*

220. *See* Lisa M. Bowman, *Napster Marches Back to Court* (July 25, 2000), *at* http://www.zdnet.com/filters/printerfriendly/0,6061,2606923-2,00.html (noting that independent surveys had indicated that Napster users were more likely to buy more CDs than people who did not sample music using file-trading systems); Laura Carr, *Stats Speak Kindly of Napster* (July 21, 2000), *at* http://www.thestandard.com/article/article_print/1,1153,17057,00.html (citing a survey that indicated that the majority of Napster users bought albums they otherwise would not have after sampling them online); Jimmy Guterman, *Why the Labels Should Love Napster* (July 24, 2000), *at* http://www.thestandard.com/ article/article_print/1,1153,16966,00.html (claiming that Napster has boosted media attention for the record industry and provides an excellent venue for labels to profit in the future); Press Release, Jupiter Research Center, Jupiter Finds Napster Users are 45 Percent More Likely to Increase Music Spending (July 21, 2000), *at* http://www.jup.com/company/pressrelease.jsp?doc=pr000721 (finding that "Napster usage is one of the strongest determinants of increased music buying"); David Segal, *Napster Looking for a Groove*, WASH. POST, July 26, 2000, at E1 (noting that Napster CEO Hank Berry has claimed that the file-trading activities of Napster's 23 million users has boosted record sales by eight percent in the first quarter of 2000).

221. *See supra* text accompanying note 184.

222. *See* Caney, *supra* note 59 (noting that Time Warner and BMG Entertainment had settled a lawsuit with MP3.com, licensing music to MP3.com for sale online); Charny, *supra* note 194 (reporting that Emusic.com offers a library of 125,000 songs for a ten dollar monthly fee with royalties paid to the labels).

223. The impact of MP3 trading to the larger music market is not relevant to a court's "potential market" inquiry. In *American Geophysical Union* the court found that the impact of copying individual articles from journals should be assessed not against the impact of the copying on sales of entire editions of the journal, but rather in respect to document delivery services, which could copy the articles and pay royalties to the copyright holders. *See* Am. Geophysical Union v. Texaco, Inc., 60 F.3d 913, 929 (2d Cir. 1995). Similarly, a court probably would find that the relevant scope of the potential market inquiry for MP3s is in fact the online trading of MP3s and not CD sales. Given this more limited scope, the purported effect of file-trading in stimulating over-the-counter sales is moot.

B. Criminal Liability for FTSs?

Criminal indictments against corporations are not as common as indictments against individuals, but neither are they rare.[224] Section 506 allows criminal charges to be brought against any "person,"[225] including, presumably, a corporation, that distributes a protected work without permission.[226] Criminal charges would probably be based on one of the forms of third party liability discussed below.

1. Contributory and vicarious criminal liability

It is unclear whether a FTS can be held criminally liable for the acts of its users. Corporations are liable for the criminal acts of their agents,[227] though courts generally prohibit vicarious liability for criminal acts.[228] The key question is whether users are agents of the FTS.[229]

In the civil suit filed against Napster, Inc., the plaintiffs alleged, *inter alia*, that Napster is liable for contributory and vicarious copyright infringement under federal law.[230] Liability for facilitating

---

224. *See* H. Lowell Brown, *Vicarious Criminal Liability of Corporations for the Acts of Their Employees and Agents*, 41 LOY. L. REV. 279, 279 (1995) (exploring the development of the law of vicarious corporate criminal liability and the judicial treatment of such actions).

225. 17 U.S.C. § 506(a) (1994 & Supp. V 1999) ("[A]ny *person* who infringes a copyright willfully . . ."). (emphasis added).

226. *Id.* § 506(a)(2).

227. *See* United States v. Automated Med. Labs., Inc., 770 F.2d 399, 406 (4th Cir. 1985) (noting that corporations may be held criminally liable in some circumstances where agents act with apparent authority of the corporation); Granite Constr. Co. v. Superior Court, 197 Cal. Rptr. 3, 9 (1983) (holding that corporations may be liable for manslaughter through their agents); People v. McArdle, 14 N.E.2d 683, 685 (Ill. App. Ct. 1938) (holding that a corporation could be held liable for criminal violation where penalty included fines); Peter J. Henning, *The Conundrum of Corporate Criminal Liability: Seeking a Consistent Approach to the Constitutional Rights of Corporations in Criminal Prosecutions*, 63 TENN. L. REV. 793 (1996) (analyzing the prosecution of criminal actions against corporations).

228. *See* State v. Guminga, 395 N.W.2d 344, 349 (Minn. 1986) (holding that vicarious liability for sales of alcohol to minors violated the State Constitution's due process clause); Davis v. City of Peachtree, 304 S.E.2d 701, 703-04 (Ga. 1983) (holding due process considerations under the state constitution required that the owner of a liquor store could not be found liable for selling alcohol to a minor where an employee of the store made the actual sale).

229. This may not be as unlikely as it may seem. Napster itself has stated that its users constitute "the system" it operates. *See* A & M Records, Inc. v. Napster, Inc., No. C 99-05183 MHP, 2000 WL 573136 (N.D. Cal. May 12, 2000). Though not employees of Napster, users perform the most important work–posting and sharing content. *See id.* Napster clearly "authorizes" its users to perform these operations, while disavowing any activities that infringe on copyright. *See id.* The trial judge in the RIAA's case against Napster, however, has alleged that "copyright infringement" is Napster's *raison d'etre*. *See id.* For a general discussion of who qualifies as a corporate agent, see Brown, *supra* note 224, at 285-89.

230. *A & M Records*, 2000 WL 573136, at *1.

criminal acts roughly parallels the civil concept of vicarious liability.[231] If a corporation is found to have "induced" a criminal act,[232] such as encouraging its employees to drive recklessly,[233] it can be found criminally liable.

Section 506 imposes criminal liability for mere distribution, regardless of financial gain,[234] but it does not address situations where a party unknowingly facilitates infringement.[235] To prevail, a prosecutor would have to show that Napster not only encourages infringement, and produces a product that enables users to infringe, but also that Napster had actual or constructive knowledge of the alleged infringement.[236]

According to Napster, the DMCA and the AHRA[237] provide it with

---

231.

> (a) Whoever commits an offense against the United States or aids, abets, counsels, commands, induces or procures its commission, is punishable as a principal. (b) Whoever willfully causes an act to be done which if directly performed by him or another would be an offense against the United States, is punishable as a principal.

18 U.S.C. § 2 (1994); *see also* AT&T v. Winback & Conserve Program, Inc., 42 F.3d 1421, 1429-32 (3d Cir. 1994) (noting and comparing the similarities between vicarious liability for trademark infringement and criminal "aiding and abetting" liability).

232. *See* 18 U.S.C. § 2(a) (1994) (describing grounds for which a principal is punishable).

233. *See* Michael Janofsky, *Domino's Ends Fast-Pizza Pledge After Big Award to Crash Victim*, N.Y. TIMES, Dec. 22, 1993, at 1 (noting that an auto accident victim alleged that the Domino's policy of giving away pizzas not delivered within a set time period may have encouraged its drivers to speed).

234. *See* Sergio G. Non, *Can Napster Survive as a Business?* (July 13, 2000), *at* http://www.zdnet.com/filters/printerfriendly/0,6061,2603462-2,00.html (questioning Napster's business model and potential profitability).

235. If third-party facilitators can be held criminally liable for aiding and abetting infringement, it is unclear whether section 512(d) affords protection from a criminal charge. Potential problems for a successful prosecution are legion, if it does apply. Napster is not obligated to police its system, and difficulties abound when determining whether the information traded on that system is "infringing." The legislative history of section 512 indicates that it exempts ISPs from contributory infringement in all cases except where it is obvious that infringement is occurring. *See* H.R. REP. NO. 105-551, pt. 2, at 45 (1998).

236. *See* Matthew Bender & Co. v. West Publ'g Co., 158 F.3d 693, 706 (2d Cir. 1998) (noting that to be found liable for contributory infringement a defendant must actively aid in direct infringement rather than merely have knowledge of the infringement (citing Cable/Home Comm. Corp. v. Network Prods., Inc., 902 F.2d 829, 845 (11th Cir. 1990))).

237. *See* 17 U.S.C. § 1001(3) (1994 & Supp. V 1999) ("A 'digital audio recording device' is any machine or device of a type commonly distributed to individuals for use by individuals, whether or not included with or as part of some other machine or device, the digital recording function of which is designed or marketed for the primary purpose of, and that is capable of, making a digital audio copied recording for private use, except for—(A) professional model products, and (B) dictation machines, answering machines, and other audio recording equipment that is designed and marketed primarily for the creation of sound recordings resulting from the fixation of nonmusical sounds."). This vague definition may allow courts to find the Napster browser a "device" within the meaning of the statute.

exemptions from either vicarious or contributory infringement liability.[238] Napster's claim essentially rests upon its allegedly passive role as a location tool, for which the DMCA provides safe harbor, and the "home taping" nature of its users activities, which the AHRA exempts from claims of infringement.[239] It remains to be seen whether either of these defenses will prove adequate in the civil suit.

The emphasis on volitional conduct in the *Netcom* ruling[240] and its statutory offspring also pose a challenge. Because the DMCA knowledge requirement practically prevents the use of imputed knowledge against third-party service providers,[241] prosecutors would most likely have to prove actual knowledge of the infringing activity.[242] The drafters of the NET Act also seem to envision an exemption for third-party facilitators who lack direct knowledge.[243]

2. Conspiracy and accomplice liability

If Napster fails to find safe harbor in the DMCA or the substantial noninfringing use doctrine, traditional approaches to multiple party criminal liability may provide an effective approach to prosecution. Two intriguing possibilities for prosecutors are charging Napster with conspiring to criminally infringe and aiding and abetting criminal infringement.

Conspiracy is defined by federal statute.[244] Prosecutors must prove that "two or more persons conspire to commit any offense against the

238. Napster claimed that it qualifies for a safe harbor under 17 U.S.C. § 512(a). Napster asserted that its system merely served a passive role as a "conduit" or router and, therefore, qualified for the protection of section 512(a) as would, theoretically, ISPs like AOL, which provide access to the Internet. *See* A & M Records, Inc. v. Napster, Inc., No. C 99-05183 MHP, 2000 WL 573136, at *1 (N.D. Cal. May 12, 2000). In denying Napster's motion for summary judgment, the court sided with the record labels, however, finding that, if Napster was a "service provider" for section 512 purposes, it was more like a search engine, similar to Yahoo!, and thus should be analyzed under section 512(d). *Id.* The court similarly dismissed the AHRA exemption for home taping as inapplicable to the facts of the case. *Id.*

239. *Id.*

240. *See* Religious Tech. Ctr. v. Netcom On-Line Comm. Serv., Inc., 907 F. Supp. 1361, 1370 (N.D. Cal. 1995) ("Although copyright is a strict liability statute, there should be some element of volition or causation which is lacking where a defendant's system is merely used to create a copy by a third party.").

241. *See* Dmitrieva, *supra* note 207, at 254-55.

242. *See generally* Robins, *supra* note 149, at 17 (arguing that the DMCA may require actual ability to control usage for ISPs to be liable for civil damages).

243. *See* 143 CONG. REC. H9883-01, H9886 (daily ed. Nov. 4, 1997) (statement of Rep. Goodlatte) ("Evidence of reproductions or distributions, including those made electronically on behalf of third parties, would not, by itself, be sufficient to establish willfulness under this act.").

244. *See* 18 U.S.C. § 371 (1994 & Supp. V 1999) (noting that the purpose of a conspiracy can be to "commit an offense" [i.e., violate a specific statute] or to "defraud").

United States . . . and one or more of such persons do any act to effect the object of the conspiracy."[245] Thus, the government must show that there is: (1) an agreement to commit a crime,[246] and (2) an overt act in furtherance of that agreement. The agreement need not be explicit; it is enough that the party charged has a "stake in the venture."[247] In *Direct Sales Co. v. United States*[248] the Supreme Court held that the agreement element could be satisfied by evidence of a tacit understanding. There, the Court found evidence that a wholesaler's sales of a prescription drug to an individual doctor far exceeded the volume of potential legitimate use was enough to establish an implicit agreement to engage in illicit activity.[249]

Napster arguably has "knowledge" that its system is used for illegal acts.[250] Napster need not "act to effect" criminal infringement, as only one party to a conspiracy must do so for all members of the conspiracy to be found guilty.[251] It would be sufficient, under the federal conspiracy statute, that the actions of users fall within the scope of Section 506.[252]

Those who facilitate the commission of a crime are held liable as principals under the federal accomplice liability statute.[253] The elements of "aiding and abetting under 18 U.S.C. § 2(a)" are "that the defendant became associated with a criminal venture and

245. *Id.*

246. In *Direct Sales Co. v. United States*, 319 U.S. 703, 713-15 (1943), the Court found the fact that sales of a prescription drug far exceeded the volume of legitimate use was enough to establish an implicit agreement to engage in illicit activity. *See also* United States v. Alvarez, 610 F.2d 1250, 1256 (5th Cir. 1980) (finding that a single indication of willingness to aid in the commission of an offense was enough to infer agreement).

247. *But see* G. Robert Blakey & Kevin P. Roddy, *Reflection on Reves v. Ernst & Young: Its Meaning and Impact on Substantive, Accessory, Aiding Abetting and Conspiracy Liability Under RICO*, 33 AM. CRIM. L. REV. 1345, 1431-32 (1996) (noting that the Supreme Court never officially adopted the "stake in the venture" requirement proposed by Judge Learned Hand, instead adopting an "intent" theory of culpability).

248. 319 U.S. 703 (1943).

249. *See id.*

250. *See* A & M Records, Inc. v. Napster, Inc., No. C 99-5183 MHP, C 00-0074 MHP, 2000 WL 1009483, at *4 (N.D. Cal. July 26, 2000) (asserting that over 85 percent of the music traded on Napster is copyrighted).

251. *See* 18 U.S.C. § 371 (1994) (where "one or more [conspirators] do any act to effect the object of their conspiracy, each shall be" punished accordingly).

252. It is also unlikely that a prosecutor would need to prove that there was explicit communication among users. *See* United States v. Bruno, 105 F.2d 921, 922-23 (2d Cir. 1938), *rev'd on other grounds*, 308 U.S. 287, 294 (1939) (finding that there was no need to prove communication between members of a drug smuggling ring where importers knew that middlemen would require the assistance of retailers and vice versa). Given the rather limited evidentiary requirements of *Direct Sales*, this might be enough to support a conspiracy conviction.

253. *See* 18 U.S.C. § 2 (1994).

participated in it . . . . Association means that the defendant shared in the criminal intent of the principal. Participation means that the defendant engaged in some affirmative conduct designed to aid the venture."[254] A prosecutor must show that the defendant acted with the intent to aid in the accomplishment of the crime,[255] merely furnishing goods used in the crime is not enough.

Napster's active creation and maintenance of an index of users, which allows criminal infringers to find material they wish to target, could fulfill the participation element. It is less certain whether a court would find that Napster shared the intent of criminal infringers. The intent necessary for accomplice liability does not always require that the aider and abetter actively desire the actual outcome of the criminal venture.[256] In some circuits, "mere knowledge" that the aid will help in the accomplishment of the crime is sufficient to satisfy the intent requirement.[257] Under this standard, Napster would most likely be found sufficiently culpable.[258]

C. Criminal Infringement and File-Sharing Software Users

Regardless of the outcome of litigation against Napster, individual users of systems like Napster may have reason to fear charges of criminal infringement.[259] Thus far, content producers such as the

---

254. United States v. Colwell, 764 F.2d 1070, 1072 (5th Cir. 1985).

255.

> [A] conspiracy also imports a concert of purpose . . . . At times it seemed to be supposed that, once some kind of criminal concert is established, all parties are liable for everything anyone of the original participants does, and even for what those do who join later. Nothing could be more untrue. Nobody is liable in conspiracy except for the fair import of the concerted purpose or agreement as he understands it; if later comers change that, he is not liable for the change; his liability is limited to the common purposes while he remains in it. The confusion is perhaps due to the fact that everything done by the conspirators—including the declarations of later entrants—is competent evidence against all, so far as it may fairly be thought to be in execution of the concert to which the accused is privy, though that doctrine too is often abused.

United States v. Peoni, 100 F.2d 401, 403 (2d Cir. 1938).

256. *See* Candace Courteau, Comment, *The Mental Element Required for Accomplice Liability: A Topic Note*, 59 LA. L. REV. 325, 328 (1998) ("[S]tandards [for the mens rea element] range from 1) mere knowledge that the accomplice's assistance will help in the commission of the offense, to 2) the accomplice's own intent to commit the offense.").

257. *See id.*

258. In one case a court seemed to suggest an ordinary sale, made with the knowledge that the buyer intended to commit a crime, would be sufficient for a finding of aider and abetter liability because of the "moral obligation to prevent the commission of a felony, if possible." *See* Backun v. United States, 112 F.2d 635, 637 (4th Cir. 1940).

259. *See* Richard Barry, *Jail Term for MP3 Pirates Predicted* (May 16, 2000), *at* http://www.zdnet.co.uk/news/2000/19/ns-15408.html (quoting a senior music

RIAA are satisfied to target companies that produce MP3 software or equipment.[260] Napster's relatively deep pockets[261] may satisfy the RIAA and aggrieved artists in civil actions. Direct infringement by individuals, however, is the *sine qua non* of infringing activity on the Napster system specifically, and among file-traders generally. Even without the FTSs, individuals using true P2P software can carry on the same activities. Record labels probably will choose to push for more aggressive criminal prosecution of individual infringers as a general deterrence strategy.[262]

A combination of factors, however, may make the criminal prosecution of individual infringers extremely complex. The most significant obstacles to prosecution will be: (1) finding a means for identifying infringers that is both technologically possible and constitutionally acceptable, (2) finding targets whose infringing activity exceeds the statutory minimum value for criminal liability, and (3) proving the *mens rea* requirement of criminal infringement.

1. Identification of criminal infringers

Identification of the accused infringers may produce the first technical and legal challenge to potential prosecution. ISPs and service providers like Napster have no duty to police their own systems to identify infringers.[263] To obtain civil relief, the RIAA, record labels, or individual artists expended their own resources necessary to seek out the infringers, including hiring private investigators to track down individual infringers.[264]

Identifying users for prosecution on criminal infringement charges

---

industry executive as proclaiming that an "individual found downloading illegal MP3 tracks" will go to jail "as a clear signal that piracy will not be tolerated in the U.S.").

260. *See* Jon O'Hara, *No-Fuss Gnutella Could Mean Napster-Sized Trouble* (June 28, 2000), *at* http://www.inside.com/story/Story_Cashed/0,2770,6280,00.html (quoting the president of the RIAA as saying that it has chosen to pursue legal action against those illegally distributing works rather than those consuming the works); Brauner, *supra* note 188, at 14 (discussing liability for third parties and "contributory conduct").

261. *See* Brad King, *Big Money Feast for Napster* (May 22, 2000), *at* http://www.wired.com/news/print/0,1294,36502,00.html (reporting a deal between venture capital firm Hummer Winblad and Napster, securing $15 million in financing for Napster).

262. *See Bernstein*, *supra* note 12, at 325-26 (arguing that the RIAA should vigorously prosecute offenders as a means of controlling infringement).

263. *See* 17 U.S.C. § 512(m)(1) (1994 & Supp. V 1999); H.R. REP. NO. 105-551, pt. 2, at 45 (1998) (stating that Section 512(d) does not require ISPs to "make discriminating judgements about potential copyright infringement").

264. *See Napster Draws Members from Lawsuit* (May 23, 2000), *at* http://www.cnet.com/news/0-1005-200-1931171.html (explaining that Napster was required under the DMCA to disable the access of users who Metallica named as likely infringers in an investigation funded by the band).

may raise much more complex legal questions than those raised by civil litigation. Government actors may face a more difficult challenge in identifying actual infringers because the evidentiary standards for a criminal conviction are stricter than in civil suits.[265] Also, the rules governing government investigations, especially search and seizure guidelines, create special limitations.[266]

When looking for targets using FTSs like Napster, government investigators may attempt to obtain information about the identity of file-traders and the content or volume of transfers directly from the FTS. Under federal law, however, a warrant must be obtained in order to compel an "electronic communication service" to disclose information about its customers or the contents of their accounts.[267] If a warrant was obtained, an FTS would probably have to divulge any relevant information about its users. It is unclear just how much information about individual users FTSs maintain.[268] Nevertheless, private investigators found ways to determine the "user IDs" of Napster users.[269]

Future prosecutions will probably not, however, involve users of systems like Napster.[270] Technologies that are more decentralized, with greater potential for copyright mayhem, will most likely replace the Napster model.[271] Identifying criminal infringers using true P2P technology presents the next challenge in enforcing intellectual property law.

---

265. *Compare In re* Winship, 397 U.S. 358, 364 (1970) ("[W]e explicitly hold that the Due Process Clause protects the accused against conviction except upon proof beyond a reasonable doubt of every fact necessary to constitute the crime with which he is charged."), *with* Rivera v. Minnich, 483 U.S. 574, 575 (1987) (finding that a preponderance of the evidence standard is appropriate for civil suits including paternity proceedings).

266. *See* Berger v. New York, 388 U.S. 41, 53 (1967) ("The basic purpose of th[e] [Fourth] Amendment, as recognized by countless decisions of this Court, is to safeguard the privacy and security of individuals against arbitrary invasions by governmental officials." (quoting Camara v. Mun. Court, 387 U.S. 523, 528 (1967))).

267. 18 U.S.C. § 2703 (Supp. V 1999) (discussing when a provider can disclose information about a subscriber to a government entity).

268. Copyright holder Metallica was able to hire a private investigation firm to determine the "usernames" of over 300,000 Napster users who it believed were specifically trading MP3s containing Metallica's material. *See* John Borland et al., *Napster May Block Hundreds of Thousands of Fans* (May 3, 2000), *at* http://news.cnet.com/news//0-1005-202-1810391.html. Napster's usernames do not by themselves, however, include the actual names or other information about particular users. *Id.* Investigators claim that they were able to determine the names of the Metallica songs shared, the time that those songs were offered for download, and the IP addresses of those offering the material. *Id.*

269. *See id.*

270. *See* Andy Oram, *Gnutella and Freenet Represent True Technological Innovation* (May 12, 2000), *at* http://www.oreillynet.com/lpt/a/208 (touting P2P Gnutella and Freenet as "a new step in distributed information systems").

271. *Id.*

Identification of these infringers will be far more difficult.[272] There is no "Gnutella, Inc."[273] With true P2P technology, finding an entity to sue for contributory infringement is probably impossible,[274] and there is no readily available source for identifying users. The hackers who have developed this software do so neither for "financial gain," nor maintain records of individuals who obtain the software.[275] It is also unlikely, primarily because of their tenuous connection to individual users, that criminal charges could be brought against these hackers under other provisions of the NET Act or DMCA.[276]

With the exception of a few companies that integrated the software into their web sites,[277] Gnutella does not provide a useful source for gathering information on individual criminal infringers.[278] Since law

---

272. *See* Robert MacMillan, *Justice Department, Rep. Coble Spar Over NET Act*, NEWSBYTES, May 12, 1999, *available at* 1999 WL 5122289 ("[P]rosecution of a crime that can be committed with 'only a $600 computer and an Internet account' are far more difficult to track down and prosecute than larger clear-cut cases of physical copyright piracy.").

273. *See* O'Hara, *supra* note 260 ("[Gnutella] isn't supported by any one individual or company, it just is.").

274. *See* Roush, *supra* note 41 (explaining the "open-source" development of Gnutella).

275. Not only does Gnutella not maintain records, but there are hundreds, perhaps thousands of Gnutella clones, or variations of the software, created by individual designers and downloaded by users. *See* Giancarlo Varanini, *On Spreading Gnutella* (Apr. 10, 2000), *at* http://music.zdnet.com/features/nerdherd/ (describing the freelance developers of Gnutella).

276. Assuming that a P2P application was found to be a circumvention device within the meaning of section 1201, criminal penalties could be brought against the designer under section 1204. Section 1204, however, retains both the willfulness and "financial gain" requirements of pre-NET Act criminal infringement liability. Therefore, it is unlikely that Gnutella and Freenet are susceptible to criminal prosecution under section 1204. For these reasons, it is likely that the RIAA and other copyright holders will push for more prosecutions of individuals on criminal infringement charges. It is doubtful that Gnutella or Freenet could be classified as anti-circumvention devices. Neither application has the capability to "descramble a scrambled work" or "decrypt an encrypted work." *See* 17 U.S.C. § 1201 (a)(3)(A0-(B) (1994); *id.* § 1201(a)(1)(A) ("No person shall circumvent a technological measure that effectively controls access to a work protected under this title."); Shahram A. Shayesteh, Note, *High-Speed Chase on the Information Superhighway: The Evolution of Criminal Liability for Internet Piracy*, 33 LOY. L.A. L. REV. 183, 219-20 (1999) (explaining the creation of a second "LaMacchia loophole" in section 1204); Kathryn Balint, *Music Won't Die When Napster Walks the Plank: Web Site Ordered Halted, but Online Piracy Thrives*, SAN DIEGO UNION-TRIB., July 28, 2000, at A1 (claiming that the recording industry's "only recourse" in fighting Gnutella and FreeNet is litigation against individuals).

277. *See* Gwendolyn Mariano, *Net Film Firm Taps Gnutella for Video Sales* (June 14, 2000), *at* http://news.cnet.com/news/0-1005-202-2080146.html (announcing the use of Gnutella by SightSound.com combined with Microsoft's digital rights management system); Jon O'Hara, *No-Fuss Gnutella Could Mean Napster-Sized Trouble* (June 28, 2000), *at* http://www.inside.com/story/Story_Cashed/0,2770,6280,00.html (citing, inter alia, Zeropaid.com, Spinfrenzy.com, and Surfy.com, as companies using Gnutella to facilitate MP3 trading on the web).

278. The developers of Gnutella keep no records identifying individual users. *See* Chris Nelson, *Digital Nation: There's Just No Stopping Gnutella* (July 30, 2000), *at*

enforcement officials cannot serve a warrant and obtain member lists or username databases from Gnutella, identification of infringers must be made through other means.

Though some touted Gnutella as a virtually invincible piracy-tool because of its supposed anonymity,[279] there are gaps that might allow law enforcement agents to identify infringers.[280] Agents might be able to detect the potentially infringing activity of Gnutella users based on the volume of transmitted material.[281] They could also log onto a network of Gnutella users and monitor the volume of downloading or uploading of various Internet Protocol (IP)[282] addresses.[283] Doing so would allow officials to find the identity of the users, as long as the ISP providing the user with Internet access agreed, or could be compelled, to divulge the account information for that IP address.[284] Given a sufficient volume, and perhaps after sampling the material offered by an uploader, agents might have enough evidence for a warrant to search and seize a suspect's hard drive.[285]

---

http://www.sonicnet.com/news/archive/story.jhtml?id=820234 (questioning the value of lawsuits directed against Gnutella, or its original "parent" company, AOL).

279. *See id.* (noting that AOL terminated the Gnutella project, created by AOL's Nullsoft division, because of fear of its use for piracy).

280. *See Future of Digital Music*, supra note 75 (statement of Gene Kan, developer and founder of Infrasearch, Inc.) ("Gnutella . . . involves no central server, eliminating the possibility of easily controlling the habits of Gnutella users by strictly legal means. *Gnutella is only pseudo-anonymous.* FreeNet corrects that. It, like Gnutella, is fully distributed with no central server, and it is completely anonymous.") (emphasis added).

281. *See* Kelly McCollum, *Student Gets 2 Years Probation in Copyright Case*, CHRON. OF HIGHER EDUC., Dec. 10, 1999, at A51 (stating that the infringing activity of University of Oregon student Jeffrey Levy was discovered when campus computer intranet administrators noticed the extremely high volume of activity on his account).

282. IP addresses are assigned to each computer when it logs onto the Internet. In some cases, individual users that access the Internet via an ISP like AOL by "dialing up" are assigned a different IP number each time. Even these "dynamic IP addresses" do not provide a method for identification, however, as ISPs assign these addresses. For more information about IP addresses, see *Find Out Your Computer's IP Address*, *at* http://www.chami.com/tips/Internet/041498I.html (last visited Aug. 16, 2000).

283. *See Gnutella Copyright Enforcement?* (June 22, 2000), *at* http://slashdot.org/articles/00/06/22/1242217.html (discussing the feasibility of identification of Gnutella users by obtaining an IP address).

284. ISPs are required to release the personal information of consumers when presented with a valid warrant. *See* 28 U.S.C. § 2703 (1994).

285. One of the important questions before magistrate judges in the future may be whether simply identifying the type of files and volume of material traded are grounds for probable cause. *See* Illinois v. Gates, 462 U.S. 213, 238 (1983) (holding that "[t]he task of the issuing magistrate is simply to make a practical, common sense decision whether, given all the circumstances set forth in the affidavit before him . . . there is a fair probability that contraband or evidence of a crime will be found in a particular place"). Trading of vast quantities of information for legitimate purposes is likely to become common place. If the hallmarks of copyright infringement become diluted by legitimate activities that possess the same traits, it may be difficult to convince a magistrate that probable cause exists. *See* United States v. Kithcart, 134

Although Gnutella may be fallible because of its divulgence of users' IP addresses, Freenet and other cutting edge file-sharing applications do not share this Achilles heel.[286] Freenet not only removes the identifying signatures from Internet traffic, it also reacts to attempted identification by distributing the data across more "nodes," creating a needle-in-the-haystack problem for investigators.[287] The International Federation of the Phonographic Industry (IFPI), a music industry "watchdog" organization, believes that Freenet poses a challenge to which there may be no solution.[288] Technological countermeasures may, nevertheless, be found.[289] However, as discussed below, fighting Freenet may come at a price society is unwilling to pay.

2. The elimination of the profit motive, the value of infringed works, and fair use

The NET Act radically altered the elements of criminal infringement when it eliminated the profit motive.[290] Section 506(a)(2) now allows prosecutors to charge an individual with criminal infringement so long as they download or upload materials with a value of more than $1,000.[291] Prior to the spread of FTSs, the

F.3d 529, 531-32 (3d Cir. 1998) (finding that the vague resemblance of two arrestees and their vehicle to the suspects in a robbery was insufficient to support probable cause for arrest given the imprecision of the description and the lack of incriminating behavior on the part of the subjects); United States v. Wilhelm, 80 F.3d 116, 120 (4th Cir. 1996) (holding that allegations corroborated only by evidence of legal activities, including a regular flow of traffic and the fact that the suspect's house contained a basement, were insufficient to support a finding of probable cause).

286. *See Features of Freenet, at* http://www.freenet.sourceforge.net/ index.php?page=features (last visited July 21, 2000) (explaining that Freenet allows both downloaders and uploaders to remain anonymous unlike Internet traffic which is labeled by IP address).

287. *Id.*

288. *See* Will Knight, *Forget Napster, Keep Tabs on FreeNet* (June 1, 2000), *at* http://www.zdnet.com/filters/printerfriendly/0,6061,2580356-2,00.html (quoting an IFPA spokeswoman, "[w]e're particularly concerned about this [technology]. It's kind of like Napster but you can't tell where information is.").

289. All technological measures are prone to countermeasures. *See* HUGO CORNWALL, THE HACKER'S HANDBOOK (1985), *available at* http://rootshell.com/docs/Hackers-Handbook (noting that technological measures like passwords may be decrypted, while other systems may be infiltrated by "trojan horses" which "consist of hiding away a bit of orthodox active code (like a virus) in a standard legitimate routine").

290. *See* Bernstein, *supra* note 12, at 326 (noting that the NET Act eliminated the commercial motive of criminal infringement).

291. These changes reflect an emphasis on harm "inflicted" on copyright holders, rather than the infringers' gain. *See* 17 U.S.C. § 506(a)(2) (1994 & Supp. V 1999) (providing criminal sanctions against infringement of copyrighted works valued at more than $1,000); 143 CONG. REC. H9883-01 (daily ed. Nov. 4, 1997) (statement of Rep. Cannon) (commenting that the bill considers harm to copyright owner and not solely on pirate's gain).

Levy case made headlines as the first successful prosecution under the NET Act, even though FBI agents could not determine the exact value of the loss caused by the infringement.[292] The relatively vast amount of data that passed through Levy's account[293] may have been sufficient as evidence to prove that his activity passed the $1,000 threshold. The failure to prove the value of the infringing material did, however, prevent Levy from being charged with a felony.[294] Similar problems related to evidence-gathering may plague prosecutions of infringers using P2P technology, but, as with Levy, proving the $1,000 minimum may not.

Technological development combined with the elimination of profit motive may make for a vast number of potential prosecutions.[295] Many Napster users could easily reach the $1,000 minimum for criminal liability, if not the $2,500 minimum[296] for felony liability. Levy operated a "warez site" or electronic Bulletin Board Service (BBS) from his university's system.[297] By comparison, using file-sharing software is far less difficult.[298] Congress has traditionally feared criminalizing widespread consumer habits in drafting copyright law.[299] Yet, such criminalization appears to be the outcome of the advent of file-sharing in the wake of the NET Act's elimination of the profit motive as an element of criminal infringement.

An average Napster user, utilizing a standard 56kbps modem,[300] can

---

292. *See* MacMillan, *supra* note 272.

293. *See* McCollum, *supra* note 281, at A51 (noting that, at one point, Levy transferred 1.7 gigabytes of data within two hours).

294. *Id.*

295. According to at least one legislator, the NET Act was already underused to prosecute criminal infringement cases in the Spring of 1999, before the advent of Gnutella and the spread of Napster-like technology. *See Implementation of the NET Act and Enforcement Against Internet Piracy, Hearing before the Subcomm. on Courts and Intellectual Property of the House Committee on the Judiciary*, 106th Cong. 1 (1999) (statement of Rep. Coble) (complaining about the lack of prosecutions under the NET Act because "there is no shortage of potential prosecutions").

296. 18 U.S.C. § 2319(c)(1) (1994 & Supp. V 1999).

297. *See* Bill Miller, *Giveaways Costly for Web Pirate: U.S. Crackdown Yields Guilty Plea*, WASH. POST, Dec. 23, 1999, at B1 (noting that Levy was the first to be convicted for operation of a "warez" site and violation of copyright laws).

298. BBSs often require the use of a pass code to gain access and are not always connected directly to the Internet. *See* G. Malkin, *Internet Users' Glossary* (Aug. 1996), *at* http://freesoft.org/CIE/RFC/Orig/rfc1983.txt.

299. *See Hearings on S. 893 Before the Subcomm. On Intellectual Property and Judicial Administration of the House Comm. On the Judiciary*, 102d Cong. 65 (1992) (statement of Edward J. Black, General Counsel, Computer & Industry Association) ("You do not want to be accidentally taking a large percentage of the American people, either small businesses or citizens, into the gray area of criminal law.").

300. Most consumers currently are using non-broadband Internet connections modems. The standard non-broadband modem connects at the rate of 56kbs (kilobytes per second). However, the trend toward the proliferation of high-speed connections will allow the transfer of increasingly enormous amounts of information

download approximately one song every eight to ten minutes.[301] Estimating that each copy of each song is worth about $1.60,[302] a Napster user would have to exchange 625 songs illicitly in order to meet the $1,000 minimum for criminal prosecution. This task could be accomplished in roughly 104 hours with a 56kbps modem. With a DSL or cable Internet connection that rate could be reduced to under twenty-six hours.[303] As standard hard drives begin to surpass twenty gigabytes in storage,[304] the requisite 1.875 gigabytes needed to store 625 songs is not difficult to attain for many computer users. Storage limitations present no legal obstacle, however, as the value of uploaded[305] works would count towards an aggregate value necessary for prosecution.[306]

Current technology does not prevent some users, however, from exceeding the minimum $1,000 worth of illicit material in an even shorter amount of time. In one notable case, the first prosecution under the NET Act, a college student was indicted for criminal infringement after campus computer operators noticed transfers of over 1.7 gigabytes in under two hours.[307] Using the powerful

---

in shorter periods of time. *See Transatlantic Cable*, WIRED, Sept. 2000, at 110 (citing a study by NetValue estimating that over 65% of American Internet users use 56K modems); *Broadband Users Mostly Young Rich Men* (June 27, 2000), *at* http://www.nua.ie/surveys/?f=VS&art_id=905355870&rel=true (citing a survey that placed broadband usage [Cable and DSL connections] among American consumers at nine percent). *But see Strategis Group Survey, US Households Eager for High-speed Access* (Feb. 18, 2000), *at* http://www.nua.ie/surveys/?f=VS&art_id=905355603&rel=true (finding that high speed access grew by 185% in the United States in 1999, and that over twenty-five million households were projected to have high speed access by 2004).

301. *See* Miller, *supra* note 40 (noting that installation of the Napster browser and downloading of three MP3s could be completed in under forty minutes).

302. This estimate is unscientific, based on the average cost of a typical ten-song album at about $16.00. Web-based retailers typically sell MP3 singles for between $1.00 and $2.49. *See* Nelson, *supra* note 278 (describing the various MP3 retailers including BMGmusicservice.com, and Emusic).

303. Though this figure is reached by extrapolating from information in previous infringement cases, including the *LaMacchia* case, the RIAA made the claim that cable modem users can download an entire one-hour compact disc in three minutes. *See NET Act Hearing*, *supra* note 119, at 146-49 (testimony of Cary H. Sherman, Senior Executive Vice President and General Counsel, Recording Industry Association of America) (discussing estimated losses to the recording industry due to piracy).

304. Even as of May 1999 average hard drive configurations gave consumers over seven gigabytes of storage. *See Market Watch: Desktop PC, Average Hard Drive* (May 1999), *at* http://www.zdnet.co.uk/pcdir/content/1999/05/marketwatch/desktops_hd.html.

305. "Uploaded" equates to "distributed" in the language of the statute. *See* 17 U.S.C. § 506(a)(2) (1994 & Supp. V 1999).

306. Section 506(a) creates liability for "reproduction or distribution." *Id.* § 506(a). Thus, anyone "downloading" (reproducing) works is liable for the value of those works combined with the value of all works "uploaded" (distributed) from his or her computer.

307. *See* Andy Patrizio, *DOJ Cracks Down on MP3 Pirate* (Aug. 23, 1999), *at*

resources of his university's intranet, the student's "typical amount of traffic" could have reached the hypothetical criminal benchmark of 625 songs in less than three hours.[308] The elimination of the "financial gain" requirement in section 506(a)(2), combined with the high-speed access of university intranets,[309] allows students to meet the value requirements for a felony conviction in an afternoon of casual "trading."

Proving that infringement reaches the $1,000 minimum in file-trading cases can be both more difficult and easier for prosecutors than in the *Levy* case. It would likely be burdensome to prove that $1,000 worth of contraband files had been downloaded or uploaded by an individual without gaining access to the target's computer hard drive, and to determine whether the target already owned authorized versions of material downloaded.[310] An individual could very easily trade the volume of material necessary to reach the $1,000 mark and exchange only non-proprietary data.[311]

Alternatively, if an individual downloaded material when he already owned an authorized version, there is a strong possibility that such activity falls within the scope of the fair use defense.[312] Investigators might discover that a high volume of material was

---

http://www.wired.com/news/news/politics/story/21391.html.

308. At an average of three minutes per song, or three megabytes of data, 625 songs could be uploaded in just over two hours with a broadband connection. *See What is MP3?*, *at* http://www.zdnet.com/zdhelp/stories/main/0,5594,2286616-2,00.html (last visited Apr. 17, 2001).

309. An intranet is "a private network that uses Internet-related technologies to provide services within an organization," like those used by universities. *See Netdictionary*, *at* http://www.netdictionary.com (last visited Feb. 16, 2001).

310. To make this determination an investigator would probably have to perform a search of the target's home, automobile, and any other place where a CD might be found. This method poses a difficult dilemma for probable cause determinations, because it would be uncertain whether the target did in fact own an authorized copy before an investigator attempted to obtain a warrant to search for unauthorized copies and it would be almost impossible to disprove the existence of authorized copies before performing a search. *See* Zurcher v. Stanford Daily, 436 U.S. 547, 556 (1978) (finding that the "critical element" in probable cause determinations "is reasonable cause to believe that the specific 'things' to be searched for and seized are located on the property to which entry is sought").

311. For example, digital files containing video or images made by an individual user (using digital still or video cameras) could be traded with others and would register as massive files, perhaps even dozens of gigabytes, and would never involve the use of copyrighted works.

312. Napster has analogized MP3s downloaded to a computer with television programs taped on a VCR. The musical works on MP3s are "space-shifted" to a computer for personal convenience, just as television programs are "time-shifted" to tape for more convenient viewing. *Compare* A & M Records, Inc. v. Napster, Inc., No. C 99-05183 MHP, 2000 WL 573136, at *3-4 (N.D. Cal. May 12, 2000) (dismissing Napster's argument that "space-shifting" is fair use), *with* Sony Corp. of Am. v. Universal City Studios, Inc., 464 U.S. 417, 418 (1984) (finding that "time-shifting" is fair use).

traded, but would never know whether the traders already owned authorized copies of that material without obtaining a search warrant. Probable cause to believe that evidence of a crime is located in a particular place is necessary for a search warrant to issue.[313] In the case of file-trading, investigators would be in the untenable position of requiring a warrant to prove the lack of exculpatory material because of the fair use doctrine.

3. "Willful" infringement

Some commentators suggest that the willfulness requirement poses an insurmountable obstacle to prosecution of criminal infringement cases.[314] Before the passage of the NET Act, the federal handbook for prosecution of intellectual property crimes noted that "amass[ing] evidence of intent in order to anticipate and rebut [the] 'lack of intent,'" or non-willfulness defense, was critical for a criminal infringement prosecution.[315] The handbook's thinly veiled skepticism towards the possibility of meeting this burden,[316] attested to by the relative paucity of criminal infringement prosecutions,[317] may not be necessary in the wake of the NET Act.

In most jurisdictions, prosecutors must prove that the accused had at least constructive knowledge of the legal duty they are charged with breaching when the *mens rea* of an offense is defined as willfulness.[318] Napster, like many other web sites, utilizes "license agreements" that include warnings about copyright violations.[319] It

313. *See infra* Part II.C.4.

314. *See* Wu, *supra* note 98, at 549-50 ("[N]otwithstanding the NET Act, which effectively eliminates the commercial motive requirement to criminalize LaMacchia-like behavior, criminal copyright enforcement remains hampered by the statutory requirement that a defendant's conduct be willful.").

315. *See* U.S. Dep't of Justice, *Federal Prosecution of Violations of Intellectual Property Rights*, *at* http://www.usdoj.gov/criminal/cybercrime/intell_prop_rts/SectIII.htm#III (updated Sept. 2, 1997) [hereinafter *DOJ Prosecution*] (discussing criminal remedies for copyright violations).

316. *Id.* ("Indeed, under this construction, if a trier of fact was satisfied that a defendant was not aware of the laws prohibiting copyright infringement, or was satisfied that the defendant did not believe his acts infringed, it might constitute a defense to the criminal charge.").

317. Currently there are only two known prosecutions for criminal infringement under the NET Act. *See* Miller, *supra* note 297, at B1.

318. *See DOJ Prosecution*, *supra* note 315 (noting that the Second and Ninth Circuits have held that willfulness requires merely an intent to copy, not an intent to act illegally); *see also* United States v. Backer, 134 F.2d 533, 535 (2d Cir. 1943); United States v. Taxe, 380 F. Supp. 1010 (C.D. Cal. 1974), *aff'd in part and vacated in part*, 540 F.2d 961 (9th Cir. 1976).

319. *See Napster License Agreement*, *at* http://www.napster.com/terms (last visited May 21, 2000) ("Napster respects copyright law and expects our users to do the same. Unauthorized copying, distribution, modification, public display, or public performance of copyrighted works is an infringement of the copyright holders'

could be argued that licenses put users on constructive or actual notice of applicable copyright law.[320]

In copyright-related cases, even law enforcement officials may lack the requisite knowledge of the law to be deemed "willful" infringers.[321] In *United States v. Moran*,[322] the defendant, a former police officer, made duplicates of copyrighted video tapes for use in his video rental store as a protection against vandalism of the originals.[323] In finding for the defendant, the U.S. District Court for the District of Nebraska noted that the relative naivete, lack of "sophistication about business matters," and misleading commentary that the defendant had read about the legality of "insuring" by making back-up copies, precluded a finding of willfulness.[324]

Like *Moran*, most Napster users, or file-sharing buffs in general, have little experience with the complexities of copyright law. Even the college and post-graduate aged adults who constitute the majority of file-sharing participants are not acquainted with copyright law at a sophisticated level.[325]

Also like Moran's "insuring" of videotapes, there is division within the media about whether "file-sharing" constitutes "fair use" or whether it is infringing activity.[326] Thus, the vast amount of press that the Napster controversy generated also could be a factor in determining whether infringement was truly willful.[327] Statistics show

---

rights.").

320. *See* ProCD, Inc. v. Zeidenberg, 86 F.3d 1447, 1455 (9th Cir. 1996) (finding that "shrinkwrap" or "end-user" licenses were valid and binding contracts).

321. *See* United States v. Moran, 757 F. Supp. 1046, 1051 (D. Neb. 1991) (holding that the test for willful infringement is the subjective belief of the defendant).

322. 757 F. Supp. 1046 (D. Neb. 1991).

323. *Id.* at 1047.

324. *Id.* at 1051.

325.

> I have complained more than once over the past few years that the copyright law is complicated, arcane, and counterintuitive; and that the upshot of that is that people don't believe that the copyright law says what it does say. People do seem to buy into copyright norms, but they don't translate those norms into the rules that the copyright statute does; they find it very hard to believe that there's really a law out there that says the stuff the copyright law says.

Jessica Litman, *Copyright Noncompliance*, 29 N.Y.U. J. INT'L L. & POL. 237, 238-39 (1997).

326. Musicians and the public are split on the question of whether trading MP3s constitutes "fair use." Only the RIAA and executives at Napster and other file-trading companies seem to have no doubts about the legality or illegality of the trading. *See* Graff, *supra* note 75, at G5 (noting the rift among musicians concerning the legality and desirability of MP3 trading); PC Data Online, *Support for Free Digital Music Echoed in PC Data Online Poll* (July 27, 2000), *at* http://www.pcdataonline.com/press/pcdo072700a.asp (noting that there is a lack of consensus among Americans about the legality of MP3 downloading).

327. The Napster web site alone has collected hundreds of articles about the case,

that most Americans are at least somewhat confused as to what constitutes an infringing use.[328] If participation is any indication of the public's position on the legality of file-sharing, the recent explosion of people engaged in file-sharing indicates an overwhelming belief that it is or should be legal.[329] It would be plausible for many infringers to claim that they did not, subjectively, believe that they were in violation of the law.[330]

4. Constitutional constraints to enforcement: The Fourth Amendment

As discussed above, the difficulty in identifying infringers is one factor that makes enforcing copyright laws against MP3 trading uniquely difficult.[331] Ironically, even if the anonymity of Freenet or Gnutella could be defeated technologically, the methods employed to do so may prove unconstitutional.

The prosecution of online copyright infringers entails special challenges for law enforcement officials, including locating and

published on the web by sources from ABC News to ZDNet.com, while an Internet search using the HotBot.com search engine of the terms Napster in conjunction with copyright yields over 600,000 hits.

328. *See* Kathryn Balint, *Music Won't Die When Napster Walks the Plank; Web Site Ordered Halted, but Online Piracy Thrives*, SAN DIEGO UNION-TRIB., July 28, 2000, at A1 (noting that recent polls indicate widespread public support for Napster and belief that trading MP3s is not infringement); PC Data Online, *supra* note 326 (citing poll statistics that 50% of Americans believed obtaining free MP3s over the Internet is or should be legal, while only 23% believed that it is illegal).

329. *See Despite Legal Woes, Napster Use Grows*, TIMES UNION, Oct. 18, 2000, at D6 (noting that the number of "unique users" (non-repeat users) on Napster soared by 345% from February to October 2000); *see also* Dick Kelsey, *Poll: Potential Jurors in Napster's Corner* (Oct. 11, 2000), *at* http://www.usatoday.com/life/cyber/nb/nb5.htm (noting that one survey found that over 41% of Americans above the age of eighteen believe that downloading music from the Internet for free is not wrong if it is for personal use).

330. *See* Mark Lemley, *Dealing with Overlapping Copyrights on the Internet*, 22 UNIV. DAYTON L. REV. 548, 577 (1997) (stating that copyright laws are not simple); Litman, *supra* note 325, at 237 (noting that common beliefs about copyright often are not in line with actual law). Almost in anticipation of this defense, the federal government and copyright holders called for copyright awareness and education programs in March 2000. *See* PRESIDENT'S WORKING GROUP ON UNLAWFUL CONDUCT ON THE INTERNET, THE ELECTRONIC FRONTIER: THE CHALLENGE OF UNLAWFUL CONDUCT INVOLVING THE USE OF THE INTERNET (2000), *available at* http://www.usdoj.gov/criminal/cybercrime/unlawful.htm#FTC (noting initiatives by the FTC, FDA, and SEC to raise awareness of Internet crime issues, including copyright violations); *Soundbyting*, *at* http://www.soundbyting.com (last visited Aug. 20, 2000) (detailing the RIAA's "Soundbyting Campaign" to raise awareness of copyright law). Were these programs to be implemented, they might undermine an *ignorantia juris* or lack of willfulness defense. If basic copyright law became common knowledge (as applied to the facts of file sharing) the factual premise of the defense would be eliminated. Regardless of whether such a program comes to fruition, it is doubtful that the willfulness requirement alone will prevent successful prosecutions. Convincing a jury ignorant of the copyright laws that the defendant was equally ignorant may not prove difficult.

331. *See supra* Part II.C.1.

seizing contraband material that exists only "on the net" for a brief time, or on personal computers.[332] Undoubtedly this would implicate the Fourth Amendment[333] guarantee of citizens' reasonable expectation of privacy.[334] When a valid expectation of privacy exists, government officials must obtain a search warrant based on probable cause to perform a search of that area or affect.[335] The Fourth Amendment also requires that warrants be issued from neutral magistrates[336] and describe the place to be searched with sufficient "particularity."[337] If there is no reasonable expectation of privacy, then the inspection is not prohibited and the evidence revealed can be submitted to a tribunal.[338] If the inspection, however, occurs without a warrant and the defendant has a reasonable expectation of privacy, the evidence is subject to the exclusionary rule.[339] The exclusionary rule prohibits the use of evidence in a criminal trial that

---

332. *See* U.S. Dep't of Justice, *Federal Guidelines for Searching and Seizing Computers*, *at* http://www.usdoj.gov/criminal/cybercrime/search_docs/sect4.htm (updated May 9, 1999) (comparing the ease of hardware searches with the difficult issues raised by searching networked computers).

333.

> The right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures, shall not be violated, and no Warrants shall issue, but upon probable cause, supported by Oath or affirmation, and particularly describing the place to be searched, and the persons or things to be seized.

U.S. CONST. amend. IV.

334. *See* Katz v. United States, 389 U.S. 347, 351 (1967) (holding that Fourth Amendment protections are limited to that which a citizen "seeks to preserve as private, even in an area accessible to the public").

335. *See id.* at 357 (noting that "searches conducted outside the judicial process, without prior approval by a judge or magistrate, are per se unreasonable under the Fourth Amendment" with few exceptions) (citing Jones v. United States, 357 U.S. 493, 497-99 (1958)).

336. *See* Coolidge v. New Hampshire, 403 U.S. 443, 449-53 (1971) (finding that a warrant issued by a state Attorney General was invalid because of the Attorney General's role as a law enforcement official); Johnson v. United States, 333 U.S. 10, 14 (1948) (stating probable cause should not to be determined "by the officer engaged in the often competitive enterprise of ferreting out crime").

337. *See* Berger v. New York, 388 U.S. 41, 56 (1967) ("The need for particularity and evidence of reliability in the showing required when judicial authorization of a search is sought is especially great in the case of eavesdropping"); United States v. Upham, 168 F.3d 532, 535 (1st Cir. 1999) (finding that a warrant's limitation to "any and all visual depictions, in any format or media, of minors engaging in sexually explicit conduct" was not too vague).

338. *See* Timothy Lynch, *In Defense of the Exclusionary Rule*, 23 HARV. J.L. & PUB. POL'Y 711, 715 (2000) (explaining how the exclusionary rule works in practice and arguing that it is constitutionally sound, because it "can be justified on separation of powers principles").

339. *See generally* Mapp v. Ohio, 367 U.S. 643, 646-60 (1961) (holding that the exclusionary rule applies to Fourth Amendment violations by states); Weeks v. United States, 232 U.S. 383, 388-98 (1914) (explaining the rationale of excluding evidence resulting from tainted searches).

was obtained in violation of the Fourth Amendment.[340] In the context of criminal infringement cases, the question is whether file-traders retain a reasonable expectation of privacy to the contents of their hard drives and their Internet communications.

Congress, courts, and the media continue to debate the privacy of Internet communications intensely.[341] Rulings addressing the Fourth Amendment protection of email[342] and the FBI's use of the email "snooping" program Carnivore[343] only raise more questions about the level of privacy that can be reasonably expected in electronic transactions.[344] The Tenth Circuit found, however, a reasonable expectation of privacy for the contents of a computer hard drive.[345]

---

340. *See* Lynch, *supra* note 338, at 714 ("Under [the exclusionary] rule, evidence obtained in violation of the Fourth Amendment is ordinarily inadmissible against a criminal defendant at trial.").

341. *See The Fourth Amendment and the Internet: Before the Subcomm. on the Constitution of the House Comm. on the Judiciary*, 106th Cong. 63-76 (2000) (statement of Robert Corn-Revere, partner specializing in Internet and telecom law, Hogan & Hartson) (noting that increasing reliance upon computers and Internet communications calls for application of Fourth Amendment protections and standards to the Internet); Richard S. Dunham, *Who's Worried about Online Privacy? Who Isn't?* (June 28, 2000), *at* http://www.businessweek.com/bwdaily/dnflash/june2000/nf00628c.htm?scriptFramed (citing a poll that found only eight percent of Americans believed their email to be "secure and private from snooping outsiders"); *Internet Users Seek Assurances Over Online Use of Personal Data*, WASH. POST, Aug. 21, 2000, at A8 (noting that surveys showed that fifty-four percent of Americans believed that "tracking" of Internet users by advertisers was harmful); Chris Oakes, *ACLU: Law Needs Carnivore Fix* (July 12, 2000), *at* http://www.wirednews.com/news/politics/0,1283,37470,00.html (noting the American Civil Liberty Union's opposition to the FBI's e-wiretapping device, "Carnivore"); John Schwartz & Robert O'Harrow, Jr., *Online Privacy Code Gets FTC's Support*, WASH. POST, July 28, 2000, at E3 (reporting that the Federal Trade Commission lauded efforts to secure the privacy of online consumers through the "Network Advertising Initiative").

342. *See* United States v. Simons, 29 F. Supp. 2d 324, 328 (E.D. Va. 1998) (holding that a government employee did not have a reasonable expectation to the privacy of his email communications on his computer system at work); United States v. Monroe, 52 M.J. 326 (C.A.A.F. 1999) (finding that a member of the United States military had no reasonable expectation of privacy to email communications on a computer owned by the federal government); United States v. Maxwell, 45 M.J. 406 (C.A.A.F. 1996) (finding that the expectation of privacy is diminished when a person uses email because it may be inadvertently read by an ISP employee or disclosed by the recipient).

343. *See* John Schwartz, *FBI Using Internet Wiretap System*, WASH. POST, July 11, 2000, at A1 (reporting that the new FBI email interception system, "Carnivore," has created controversy and fears about Fourth Amendment violations).

344. *See generally* Edward Fenno, *Federal Internet Privacy Law*, 12 S.C. LAW. 36, 38 (2001) (noting that "since many Internet privacy issues are still relatively new, the law in the area is in a state of flux"); Michael Adler, Note, *Cyberspace, General Searches, and Digital Contraband: The Fourth Amendment and the Net-Wide Search*, 105 YALE L.J. 1093, 1109 (1996) (arguing that the growing reliance on computers as "diary . . . date book . . . [and] checkbook" necessitates finding a reasonable expectation of privacy to the contents of computers in order to preserve fundamental liberties).

345. *See* United States v. Campos, 221 F.3d 1143, 1148 (10th Cir. 2000) (requiring officers to obtain warrants to search the contents of hard drives and further requiring officers to "engage in the intermediate step of sorting various types of

Though courts seem to concede that persons have a right to privacy concerning the contents of hard drives generally,[346] Fourth Amendment precedent suggests that file-traders may not have the same blanket expectation of privacy.[347] As the act of file-sharing enables traders to search one another's hard drives for material they are interested in uploading,[348] one could argue that file-traders "open the box" by trading files, and that the users' expectation of privacy is nullified.[349]

Legitimate Internet usage can, and increasingly will, entail the transfer of large amounts of data,[350] therefore determining whether the content of file-trading activity is contraband will require more than observing the "heavy traffic" that led investigators to Jeffrey Levy.[351] Where it is technologically possible, the large quantity of legal Internet traffic may mean agents will be forced to either intercept file-trading traffic to determine content,[352] or remotely

---

documents and then only search the ones specified in a warrant") (*citing* United States v. Carey, 172 F.3d 1268, 1271 (10th Cir. 1999)).

346. The Electronic Communications Privacy Act contains criminal provisions that indicate a strong legislative intent to safeguard the privacy of electronic data stored in computers. *See* 18 U.S.C. § 2701 *et seq.* (1994 & Supp. V 1999); *see also* Davis v. Gracey, 111 F.3d 1472, 1478 (10th Cir. 1997) (noting in the context of a search of the defendant's hard drive that the "'Fourth Amendment requires that a search warrant be seized with sufficient particularity'" (quoting Voss v. Bergsgaard, 774 F.2d 402, 404 (10th Cir. 1985))); United States v. Lyons, 992 F.2d 1029, 1031 (10th Cir. 1993) (finding that the expectation to privacy in the contents of a hard drive is subject to the society's recognition of that expectation (citing Minnesota v. Olson, 495 U.S. 91, 95 (1990))). *But see* United States v. Kennedy, 81 F. Supp. 2d 1103, 1110 (D. Kan. 2000) (holding that a person has no privacy interest in Internet subscriber information maintained by an ISP).

347. The Supreme Court held that "a person has no legitimate expectation of privacy in information he voluntarily turns over to third parties." *See* Smith v. Maryland, 442 U.S. 735, 743-44 (1979) (finding that the use of a "pen register" device to determine the telephone numbers called by the defendant was not a search).

348. *See* Borland, *supra* note 214 (noting the vulnerability of information on the computers of Napster and Gnutella users).

349. Under the Katz "reasonable expectation of privacy" test, police are free to make a search outside the protections of the Fourth Amendment when the search is one that members of the public could make without the consent of the defendant. *See* United States v. White, 401 U.S. 745, 752 (1971) (finding that "one contemplating illegal activities must realize and risk that his companions may be reporting to the police"); United States v. Meriwether, 917 F.2d 955, 958-60 (6th Cir. 1990) (holding that by placing a call to another member of the public via a pager, the defendant had assumed the risk that authorities would intercept the information).

350. *See Transatlantic Cable*, *supra* note 300, at 110 (citing statistics that show average American and French Internet users downloading activity has grown to almost 200 Megabytes every month); Scott Rosenberg, *The Napster Files* (Feb. 4, 2000), *at* http://www.salon.com/tech/ col/rose/2000/02/04/napster_swap/print.html (stating that standard personal computer hard drives are estimated to hold 1,000 Gigabytes of data by 2005).

351. *See* McCollum, *supra* note 281, at A51.

352. "Packet-sniffer" network tools can at least determine the kind of file being

search the hard drives of suspects.[353] One possibility is that agents will simply connect to file-traders in "undercover" operations disguised as fellow file-traders and gain access to hard drives using Freenet or Gnutella as a vehicle.[354]

One might argue that private investigators could uncover evidence of Internet piracy, avoiding constitutional constraints that are imposed on government agents.[355] Government solicitation of this behavior, however, would legally transform these private actors into government agents, precluding any evidence gathered in violation of Fourth Amendment protections.[356] Though this point is arguable, it is probably enough to note that a degree of private and government cooperation in this area will, at the very least, lead to substantial ethical and evidentiary problems.

The remaining difficulty, however, is determining whether users are in fact be engaged in fair use.[357] Even if MP3 files containing copyrighted works are found, there is no way for an investigator to

---

transmitted, such as those carrying the ".mp3" tag. More sophisticated interception methods may be developed in the future. *See Packet Sniffer*, *at* http://www.sinica.edu.tw/cc/course/unix-overview/ node26.html (last visited Apr. 17, 2001) (explaining the technical specifications of "packet sniffers").

353. A hypothetical example might be as follows: suppose that Bob is a student at Big State University. Bob uses both computers attached to the university's system as well as his own home computer which is connected to the Internet via a dial-up ISP and a cable modem. Bob actively trades MP3 files using Freenet. Bob's trades are conservatively estimated at around $1,000 in value every month. Bob has heard of some legal disputes about MP3 trading, but no one seems to agree whether it is legal or not. Bob decides to "keep on truckin'." First, just "finding" Bob's illicit activity presents problems. Agents probably do not know where to start looking, unless they engage in a "sting" by luring Bob to trade files and are somehow able to defeat Freenet's anonymity protections to identify his computer. Unless Bob traded enough material just with the agents' computers, however, the agents still would not know whether Bob's trading surpassed the criminal threshold. University computer system operators might notice large volumes of material passing through Bob's system, but as legitimate transfers of large quantities of data become more common, it is doubtful whether the transfers would constitute adequate suspicion, or be grounds for a search of Bob's computer. Obtaining a warrant without the help of information from the sting operation would be difficult in this scenario, and the sting might raise the problem of defeating an entrapment defense.

354. *See* Healey, *supra* note 75 (noting that the developer of Zeropaid.com used Gnutella to "sting" child pornography traders by posting files with suggestive names and then publishing the Internet addresses of those who download them).

355. *See Napster Draws Members from Lawsuit* (May 23, 2000), *at* http://www.cnet.com/news/0-1005-200-1931171.html?tag=st.cn.sr.ne.1 (explaining that Metallica was successful in identifying infringers in a private investigation funded by the band).

356. *See* Skinner v. Ry. Labor Executives' Ass'n, 489 U.S. 602, 615-16 (1989) (holding that a railway was a government actor where it administered drug tests under government regulations that showed a "strong preference" for the tests); United States v. Walther, 652 F.2d 788, 792-93 (9th Cir. 1981) (finding that an airline employee acted as government agent where he acted under expectation of D.E.A. reward).

357. *See* discussion *infra* Part I.B.5.b.

verify whether the target also owns an authorized copy of the work, perhaps in a format like compact discs, which would make the MP3 file a legitimate fair use copy. Distribution of that copy would constitute infringement,[358] but gathering evidence of distribution exceeding the criminal threshold might be difficult, and complicated further still by the entrapment defense, discussed below.

5. Entrapment

The most promising method currently available for discovering the identity of criminal infringers may also provide targets with an additional defense. By using the undercover methods described above,[359] and posing as file-traders offering works for trade in order to gain access to infringers' hard drives to discover contraband, police may allow the infringers to raise the defense of entrapment.[360] To succeed the defendant must show: (1) that the government agents induced the commission of the crime, and (2) that the defendant was not predisposed to commit the crime.[361]

In a file-trading "sting" it would be impossible for defendants to claim that the government induced them to engage in file-trading, since one would already have to be engaged in active trading to become a target. Defendants, however, need only prove that they were induced to upload or download works with an aggregate value that exceeds the criminal threshold.[362] Inducement will be found if

358. *See* 17 U.S.C. § 106(3) (1994) (granting copyright owners the right of distribution); *id.* § 501 (making a violation of the distribution right, *inter alia*, actionable as infringement).

359. *See also* Jennifer Gregg, Note, *Caught in the Web: Entrapment in Cyberspace*, 19 HASTINGS COMM. & ENT. L.J. 157, 186-93 (1996) (discussing the law of entrapment and its application in Internet crime cases, especially those involving child pornography).

360. *See generally* Ronald J. Allen et al., *Clarifying Entrapment*, 89 J. CRIM. L. & CRIMINOLOGY 407, 409 (1999) (reviewing entrapment jurisprudence and arguing that the "predisposition" element is a "fictional entity," and that, since it does not exist either no one is predisposed to commit the crime, or "everyone . . . is predisposed to commit the crime").

361. *See* Jacobson v. United States, 503 U.S. 540, 549 (1992) (holding that the burden is upon the government to show predisposition but declining to define a bright line test); United States v. Dunn, 779 F.2d 157, 160 (2d Cir. 1985) ("Furthermore, in order to reach the central issue of predisposition, we have held that there need only be some evidence of government initiation of the illegal conduct." (citing United States v. Martinez-Carcano, 557 F.2d 966, 969-70 (2d Cir. 1977))). A defendant either has the burden of production or must prove entrapment by a preponderance of the evidence, depending upon the jurisdiction. *See* United States v. Damblu, 134 F.3d 490, 492 (2d Cir. 1998) ("Entrapment is a defense for which the defendant bears the burden of proof by a preponderance of the evidence."); State v. Smith, 677 P.2d 100, 103 (Wash. 1984) (noting that the defendant has the burden of production in raising a defense of entrapment).

362. The defense must make the distinction that the defendant engaged in conduct that, while similar, was not criminal, and that it was the government that

government agents conducting the sting initiated the illegal conduct, regardless of whether "pressure tactics" are used.[363]

Proving that the predisposition element is in their favor may be more difficult for the defense. Prosecutors can argue that the fact that the defendants engaged in file-trading, though not dispositive, is strong evidence of a willingness to act criminally. In cases where there is evidence of *some* infringing activity before government involvement, prosecutors will have a strong argument that the government only provided an opportunity for the defendants to act on their criminal inclinations, in which case entrapment is not a defense.[364] If defendants, however, can show that their file-sharing tendencies were not *criminal* tendencies until the government produced a fatal temptation, entrapment may provide a complete defense.[365]

6. Jurisdiction

American courts have responded with flexibility when faced with determining jurisdiction for acts that take place in cyberspace.[366] Finding jurisdiction over Internet crimes is not difficult when the culprits are to be found on American soil.[367] But the threat to

initiated or solicited the criminal actions. *See* United States v. Mayo, 705 F.2d 62, 67-70 (2d Cir. 1983) (explaining the entrapment defense).

363. *See Dunn*, 779 F.2d at 158 ("In this circuit, 'soliciting, proposing, initiating, broaching or suggesting the commission of the offence charged' does constitute inducement." (citing United States v. Sherman, 200 F.2d 880, 883 (2d Cir. 1952))); United States v. Riley, 363 F.2d 955, 958 (2d Cir. 1966) (stating that inducement does not depend on "the degree of pressure exerted").

364. *See Martinez-Carcano*, 557 F.2d at 970 ("[T]he Government has to prove beyond a reasonable doubt that the defendant was ready and willing to commit the crime." (quoting United States v. Braver, 450 F.2d 799, 805 (2d Cir. 1971))).

365. *See* Catherine Shultz, Note, *Victim or the Crime?: The Government's Burden in Proving Predisposition in Federal Entrapment Cases*, 48 DEPAUL L. REV. 949, 966 (1999) (noting that current entrapment jurisprudence places the burden of proof on the prosecution to show that the defendant was predisposed to commit the crime beyond a reasonable doubt and precludes "the defendant's ready response to the government solicitations cannot be enough to establish that he was predisposed to commit the crime").

366. *See* Kevin J. Smith, *Internet Taxes: Congressional Efforts to Control States' Ability to Tax the World Wide Web*, 7 RICH. J.L. & TECH. 3, ¶ 62-64 (2000), *at* http://www.richmond.edu/jolt/v7i1/article3.html (collecting cases and noting that courts have developed a rough test for finding personal jurisdiction in Internet cases, recognizing that the simple ability to view a website is not enough to support jurisdiction, and inquiring whether the Internet activity was passive and whether it was directed in any particular way at the forum state); *see also* Inset Sys., Inc. v. Instruction Set, Inc., 937 F. Supp. 161, 164-65 (D. Conn. 1996) (finding jurisdiction over a company due, in great part, to its use of the Internet to solicit business in the forum state).

367. So long as the defendant's actions are directed towards a particular forum, such that he reasonably may expect to haled into court there, a court is likely to find jurisdiction. *See Inset Sys.*, 937 F. Supp. at 165; Clyde H. Wilson, Jr. & M. Susan

copyright is not limited to the boundaries of the United States.[368]

The global nature of the Internet promises to make enforcement of copyright law even more challenging.[369] Some e-commerce entrepreneurs have recently taken the step of placing their systems on a World War II era anti-aircraft platform in the North Sea in an effort to avoid the complications imposed by falling within the jurisdiction of any sovereign nation.[370] Hunting down copyright bandits from Belize to Tanzania, not to mention the open seas, might be a challenge too great even for the long-arm of American law. A full analysis of the jurisdictional problems posed by the international nature of the Internet is beyond the scope of this Comment.

CONCLUSION

Increased pressure by copyright holders and content industry associations may bring about more prosecutions of FTS users for criminal infringement of musical recordings and other protected works. The current legal regime criminalized a very common behavior. Prosecuting these crimes will not be without significant hurdles. Chief among those constraints will be questions about the constitutionality of evidence-gathering techniques on the Internet and computer users' reasonable expectations of privacy. Congress, the courts, and society must decide what price we are willing to pay to protect the rights of intellectual property producers and owners, and whether sacrificing a significant amount of privacy for this objective is worth the cost. Yet, even deciding to forego some privacy may not be enough to allow for successful prosecutions and stem the tide of copyright infringement. The Internet's global nature and the lack of international consensus on the contours of legitimate intellectual property right promises many criminal infringers shelter beyond our borders.

Whatever the outcome of the legal debate, the progress of

Wilson, *Cyberspace Litigation: Chasing the Information Highway Bandits*, TRIAL, Oct. 2000, at 48 ("The key seems to be the degree of interactivity. A site permitting individual purchases, without more, is probably inadequate to confer personal jurisdiction, but a site soliciting a subscription relationship with customers for a continued supply of information is probably adequate to confer jurisdiction.").

368. *See generally* Symposium, *Panel III: Intellectual Property Issues in E-Commerce—Piracy in the Internet Age*, 17 ARIZ. J. INT'L & COMP. L. 131 (2000) (noting that piracy is a rampant problem and that the international nature of the Internet only heightens intellectual property law enforcement problems).

369. *See* Simson Garfinkel, *Welcome to Sealand. Now Bugger Off.*, WIRED, July 1, 2000, at 230 (reporting that some Internet entrepreneurs have purchased an aging anti-aircraft deck in the North Sea, which they intend to turn into an extra-territorial oasis for Internet rebels called "Sealand").

370. *Id.*

technology will probably ensure that copyright infringement will continue to plague content industries while remaining a source of entertainment for technophiles. Technology, rather than innovative use of existing laws, will probably prove to be the key, if there is any, to protecting intellectual property. If investigators are able to find a way to discover "illicit" copies without the currently necessary intrusion into the inner sanctums of private information stored on our computers, copyright owners will be able to sleep a little better. In the end, permanently preventing the development of anonymity-protecting file-sharing software will probably be impossible. As one dot-com CEO has noted, "[t]he only way to stop [Gnutella] is to turn off the Internet."[371]

371. Franklin Paul, *Internet Music Debate Moves to Washington* (May 24, 2000), *at* http://www.cnn.com/2000/LAW/05/24/mp3.napster.suit/index.html.