

# UIC John Marshall Journal of Information Technology & Privacy Law

---

Volume 18  
Issue 3 *Journal of Computer & Information Law*  
- Spring 2000

Article 4

---

Spring 2000

## RIAA v. Napster: A Window onto the Future of Copyright Law in the Internet Age, 18 J. Marshall J. Computer & Info. L. 755 (2000)

Ariel Berschadsky

Follow this and additional works at: <https://repository.law.uic.edu/jitpl>



Part of the [Computer Law Commons](#), [Entertainment, Arts, and Sports Law Commons](#), [Intellectual Property Law Commons](#), [Internet Law Commons](#), [Privacy Law Commons](#), and the [Science and Technology Law Commons](#)

---

### Recommended Citation

Ariel Berschadsky, RIAA v. Napster: A Window onto the Future of Copyright Law in the Internet Age, 18 J. Marshall J. Computer & Info. L. 755 (2000)

<https://repository.law.uic.edu/jitpl/vol18/iss3/4>

This Article is brought to you for free and open access by UIC Law Open Access Repository. It has been accepted for inclusion in UIC John Marshall Journal of Information Technology & Privacy Law by an authorized administrator of UIC Law Open Access Repository. For more information, please contact [repository@jmls.edu](mailto:repository@jmls.edu).

# RIAA v. NAPSTER: A WINDOW ONTO THE FUTURE OF COPYRIGHT LAW IN THE INTERNET AGE

by ARIEL BERSCHADSKY†

## TABLE OF CONTENTS

I. OVERVIEW .....	756
II. MUSIC AND THE INTERNET .....	758
III. THE BIRTH OF NAPSTER .....	759
IV. RECORDING INDUSTRY ASSOCIATION OF AMERICA'S LAWSUIT AGAINST NAPSTER .....	762
V. COPYRIGHT LAW IN THE DIGITAL AGE .....	763
A. BACKGROUND .....	763
B. BASIC FORMS OF COPYRIGHT INFRINGEMENT .....	764
1. <i>Direct Liability</i> .....	764
2. <i>Contributory Liability</i> .....	765
3. <i>Vicarious Liability</i> .....	766
C. ONLINE COPYRIGHT INFRINGEMENT LIABILITY LIMITATION ACT (TITLE II) .....	767
1. <i>Title II Internet Service Provider Status</i> .....	768
2. <i>Title II Functional Safe Harbors</i> .....	768
a. <i>Transitory Digital Network Communications (Conduit)</i> .....	768
b. <i>System Caching</i> .....	768
c. <i>Information Residing on Systems at Direction of Users (User Storage)</i> .....	769
d. <i>Linking to Infringing Material Via Information Location Tools</i> .....	769
VI. NAPSTER'S LEGAL LIABILITY .....	770

---

† Ariel Berschadsky received a BS in Development Economics from the Georgetown University School of Foreign Service, an MBA in Finance and Operations Research from the University of Chicago Graduate School of Business, and a JD from the Georgetown University Law Center. He will be an attorney in the Corporate Division of White & Case in New York commencing in October 2000. The author wishes to thank Professor Laura Underkuffler of Duke University for her helpful comments.

A.	DIRECT COPYRIGHT INFRINGEMENT BY NAPSTER'S USERS.....	770
B.	ASSESSMENT OF NAPSTER'S CONTRIBUTORY LIABILITY .	771
C.	ASSESSMENT OF NAPSTER'S VICARIOUS LIABILITY .....	774
D.	NAPSTER'S PROTECTED STATUS UNDER TITLE II .....	775
	1. <i>Napster's Internet Service Provider Status</i> .....	776
	2. <i>Napster's Protected Function Status</i> .....	776
	a. <i>Napster as a Transitory Digital     Communications Network</i> .....	776
	b. <i>Napster as a Provider of System Caching</i> ....	777
	c. <i>Napster as a Provider of User Storage</i> .....	777
	d. <i>Napster as an Information Location Tool</i> ....	778
	(i) <i>Knowledge of Copyright Infringement</i> ....	778
	(ii) <i>Removal of Infringing Material Upon         Knowledge of Infringement</i> .....	780
	(iii) <i>Direct Financial Benefit from Copyright         Infringement</i> .....	781
	(iv) <i>Removal of Infringing Material Upon         Notification of Infringement</i> .....	781
E.	LEGAL CONCLUSION: NAPSTER'S ACTIVITIES ARE PROTECTED BY TITLE II .....	782
VII.	IMPLICATIONS FOR THE FUTURE .....	782
A.	TECHNOLOGICAL CAT AND MOUSE GAME .....	782
B.	PARADIGM SHIFT IN THE MUSIC INDUSTRY.....	785
	1. <i>Low-Priced Distribution with Convenient     Purchasing</i> .....	786
	2. <i>Mass Customization</i> .....	787
	3. <i>Advertiser-Support</i> .....	788
	4. <i>Record Companies as Information Providers</i> .....	788
VIII.	CONCLUSION .....	789

## I. OVERVIEW

Few areas of law have been as affected by the dawn of the Internet age as copyright law. The ease and speed with which copywritten material can be transmitted through cyberspace makes detection and termination of copyright violations a daunting task. Legislative efforts to adapt copyright law to the new realities of the Internet have been outpaced by the rapid transformation of software and hardware technology, which permits the circumvention of existing legal mechanisms designed to protect intellectual property rights.

One of the industries most concerned about the Internet's impact on intellectual property rights is the music and recording industry ["the music industry"]. Its main representative, the Recording Industry Associa-

tion of America ("RIAA"),<sup>1</sup> has expended substantial energy over the last few years to identify and combat Internet-based music piracy.<sup>2</sup> But the RIAA now faces the greatest challenge of its 48-year history, a challenge made particularly remarkable by the fact that it has come from a fledgling Internet company founded just over a year ago by a nineteen-year-old. This company, Napster, facilitates the process by which music files can be located and downloaded electronically and, in so doing, has the potential to radically transform the business paradigm under which the music industry currently operates.

The RIAA has responded to the Napster threat by helping several record companies file suit against Napster, alleging contributory copyright infringement and vicarious liability for copyright infringement.<sup>3</sup> The RIAA's lawsuit, which was filed on December 9, 1999, touches upon the gray area of copyright law that tries to strike a balance between protecting intellectual property in cyberspace while shielding Internet Service Providers (ISPs) from liability for the unauthorized actions of their users. As such, the resolution of this case has far-reaching implications for the future of property rights in cyberspace, even beyond the music industry. Television and film companies correctly view the Napster dispute as a glimpse into their own future.<sup>4</sup> Presently, high-quality video files are too large to be sent quickly over most Internet connections, but faster transmission services will soon threaten the *status quo* in their industries as well.<sup>5</sup>

This paper will use the Napster controversy as a platform from which to discuss a fascinating new technology and to better understand

---

1. The RIAA represents 90% of the music industry and is responsible for the licensing and sale of music materials. See RIAA, *Frequently Asked Questions* (last modified May 26, 2000) <<http://www.riaa.com/About-Who.CFM>>.

2. See Don Clark, *Recording Industry Group Sues Napster, Alleging Copyright Infringement on Net*, WALL ST. J., Dec. 9, 1999, at B18, available in 1999 WL 24925087.

3. See *A&M Records v. Napster, Inc.*, No. 99-5183 (N.D. Cal. filed Dec. 6, 1999). In this lawsuit, the RIAA is assisting the record companies A&M Records, Geffen Records, Interscope Records, Sony Music Entertainment, MCA Records, Atlantic Recording Corp., Island Records, Motown Record Co., Capital Records, La Face Records, BMG Music d/b/a/ The RCA Records Label, Universal Records, Elektra Entertainment Group, Arista Records, Sire Records Group, Polygram Records, Virgin Records America, and Warner Bros. Records. *Id.*

4. Benny Evangelista, *Entertainment Companies are Alarmed by Online Programs that Let Anyone Copy Music and Movies*, THE SAN FRANCISCO CHRONICLE, Apr. 3, 2000, at E1 (noting the development of DivX, a program that can copy and compress a full-length DVD film into a file that can fit onto a standard 650 MB CD-ROM).

5. See Amy Harmon, *Potent Software Escalates Music Industry's Jitters*, N.Y. TIMES, Mar. 7, 2000, at A1; David Weekly, *Three Days of MIRC* (visited Apr. 27, 2000) <<http://david.weekly.org/writings/mirc.php3>> (noting that MIRC, an Internet Relay Chat system, already enables sophisticated Internet users to transfer video files); See also Evangelista, *supra* note 4, at E1.

copyright law in the Internet age. The Overview is followed by a brief discussion of music piracy over the Internet in Section II. Section III discusses why Napster came into being and how it functions. Section IV discusses the specific allegations of copyright infringement made against Napster by the RIAA. Section V provides a brief overview of copyright law, various forms of copyright infringement, and how copyright law has been adapted to the new challenges posed by the Internet. Section VI then considers the legal merit of the RIAA's allegations. Section VII discusses the implications of technological change for the music industry, and Section VIII offers a brief conclusion.

## II. MUSIC AND THE INTERNET

Until just a few years ago, a music lover on a tight budget generally had to sacrifice sound quality. Unless he was willing to listen only to what was on the radio at that moment, he was relegated to listening to relatively inexpensive records or cassettes, analog-based mediums that deteriorate with each subsequent playback. For those demanding the high sound quality and longevity of digitally recorded music, and willing to pay for it, CDs were the medium of choice.

Though the prices of CDs have remained high over time,<sup>6</sup> the price of computer technology has decreased steadily over the past decade. As a result, today about 60 million American households own personal computers and 43 million households have Internet access.<sup>7</sup> With such widespread access to digitally-based information combined with the increasing use of computers for entertainment, it was only a matter of time before music began to be transmitted through cyberspace.

The transmission of music over the Internet began in earnest with the introduction of the World Wide Web and the browser in the early nineties, but was initially hampered by slow transmission speeds.<sup>8</sup> Downloading a five-minute song could easily take several hours given the characteristics of telephone lines, which limited most Internet connections to a speed of 56,000 bauds per second (56K).

Eventually, the MP3 compression algorithm was developed,<sup>9</sup> and it

---

6. See *Retailer Profile*, National Ass'n of Recording Merchants (visited Apr. 27, 2000) <<http://www.narm.com/programs/research.htm>> (providing data for the average dollar sale of audio products, primarily CDs, relative to the number of items purchased, for the period 1992 through 1998).

7. See Katherine Yung, *America Joins Trend: Home PCs*, DALLAS MORNING NEWS, Mar. 2, 2000, at 1A, available in 2000 WL 14657422.

8. See Hamish McRae, *The Markets May be Mad, But They May Also be Profoundly Wise*, THE INDEP. - LONDON, Mar. 9, 2000, at 4, available in 2000 WL 6464248.

9. See *MP3 Site Ties Up With Local Record Company*, PHILIPPINE DAILY INQUIRER, Apr. 3, 2000 at 7. MP3 is the acronym for Moving Picture Experts Group 1, Audio Layer 3.

is now the most popular format for downloading music.<sup>10</sup> The widespread use of MP3 files stems from the fact that they are highly compressed yet provide near-CD sound quality.<sup>11</sup> Transmission of MP3 files over the Internet is substantially quicker than it is with older, space-consuming formats such as WAV. Furthermore, as with any digital format, MP3 files can be copied and distributed an unlimited number of times without degrading their sound quality. But despite the ease of transmitting an MP3 file, the tough part has been to locate specific ones in the vastness of cyberspace—at least until now.

### III. THE BIRTH OF NAPSTER

In early 1999, Shawn Fanning, a nineteen-year-old freshman computer science student at Northeastern University, wanted to make it easier for his roommate to find MP3 files over the Internet.<sup>12</sup> Finding a specific MP3 file, then as now, is generally a tedious process. Using a search engine such as Lycos or Yahoo, a person obtains a list of websites supposedly containing the desired file, and then enters each site individually to determine if it contains a downloadable copy. Often the web link provided by the browser is invalid due to the website being closed or temporarily off-line (i.e., a “dead link”). Occasionally the web link is a ruse designed to direct people to lewd material. Other times, an appropriate web site may be found, but the files it contains are disorganized or are transmitted slowly. An alternative to using a search engine is to find someone willing to send the desired file via e-mail.<sup>13</sup> Either approach is time-consuming.

Fanning’s solution was simple, yet elegant: enable people to share MP3 files on their hard drives directly with one another with the assistance of a centralized database of titles combined with software that converts each user’s computer into a server. Based on this conceptual breakthrough, in a matter of months Fanning had developed a system he

---

10. See Julian Dibbell, *The Record Industry’s Digital Daze*, ROLLING STONE, Nov. 26, 1998, at 106, available in 1998 WL 27734514 (estimating 5 million users worldwide).

11. See *A&M Records v. Napster, Inc.*, No. 99-5183 (N.D. Cal. filed Dec. 6, 1999), at para. 41. MP3 files take up only one-twelfth the space of a typical music file; see also Telephone Interview with Konstantin Läufer, PhD, Associate Professor of Computer Science, Loyola University - Chicago (Mar. 16, 2000). The compactness of an MP3 file is achieved by removing inaudible elements and then algorithmically compressing what remains. The perceived frequency response and signal-to-noise ratios are retained. *Id.* This is known as “lossy” compression. *Id.*

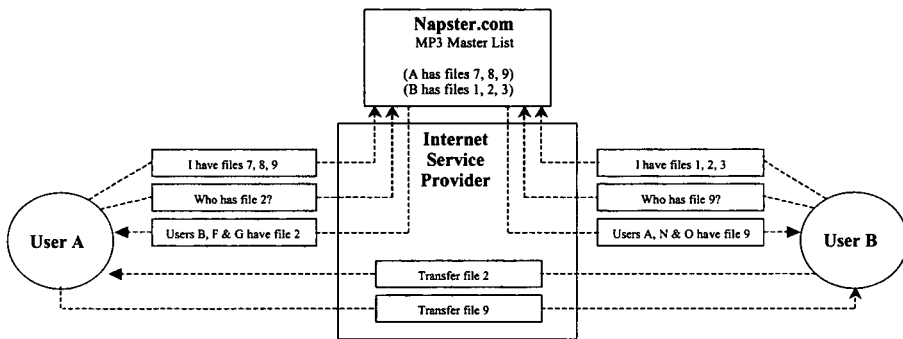
12. See Harmon, *supra* note 5, at A1.

13. See *id.* This can entail persuading the provider, if he does not already have the desired song on his hard drive, to “rip” (i.e., convert) the music from a CD into a file on his hard drive before he can e-mail it. *Id.* The ripping software is freely available over the Internet. *Id.*

named Napster.<sup>14</sup> The software component of the system, MusicShare, enables a user to connect to a database located at the Napster website and tell it which MP3 files he is willing to share with other Napster users. The names of these MP3 files as well as the Internet Protocol (IP) address for each "Host" user are then stored in Napster's central database. This list is continually updated as Hosts log on or off.<sup>15</sup> The files themselves are never stored on Napster's servers.

Any Napster user can connect to this central database to search for a specific title. Within a few seconds the user is told whether there are any Hosts offering this title, the different recording qualities ("bitrates") that are available, the file sizes, and each Host's line speed. The user specifies from which Host he wishes to download the MP3 file. A message is then transmitted through Napster's servers to the appropriate Host, which assumes the role of server and immediately begins transferring the file directly to the user through each party's respective ISP.<sup>16</sup> From this point forward, Napster's website is out of the picture.<sup>17</sup> This process is depicted in the diagram below.

### Napster Operating Model



14. See Warren Cohen, *Napster is Rocking the Music Industry*, U.S. NEWS AND WORLD REP., Mar. 6, 2000, at 41, available in 2000 WL 7717576 (explaining that "Napster" was the nickname given to Mr. Fanning when he let his closely cropped hair grow a bit shaggy).

15. See *Pl.'s Mem. of P. & A. in Opp'n. to Def. Napster, Inc.'s Mot. for Summ. Adj. on the Applicability of the 17 U.S.C. § 512(a) Safe Harbor Affirmative Defense* (N.D. Cal. 2000) (No. C99-5183), at 10 [hereinafter *Pl.'s Opp'n to Napster's Mot. for Summ. Adj.*].

16. See Telephone Interview with Sean Parker, Product Development, Napster, Inc. (Mar. 23, 2000) [hereinafter *Parker Interview*].

17. See *A&M Records v. Napster, Inc.*, No. 99-5183 (N.D. Cal. filed Dec. 6, 1999), at para. 50. At the time the RIAA filed its lawsuit, Napster stayed involved in the entire download process to ensure that file transmission was completed successfully. *Id.* If a download was interrupted because, for example, the user offering the file had logged off, Napster would automatically locate the same recording from another Napster user and resume the download at the point it was interrupted. *Id.* This feature was disabled in January 2000. *Id.*

Napster thus functions as a community of MP3 listeners. Though most Napster users are willing to share their MP3 files, any Napster user can deny access to his files while retaining the ability to download from other users.<sup>18</sup> A major advantage of Napster over traditional search engines is that by specializing in MP3 files, and by possessing a continually updated database of file names, it is nearly certain that a user seeking a specific file will be able to successfully transfer it if it is listed in the Napster database.<sup>19</sup>

Realizing that his system had enormous commercial potential, Fanning incorporated Napster in May 1999 and made his software freely available to the public that August.<sup>20</sup> Currently, the company is operating on venture capital, but it may obtain its future revenue from advertising, subscriber fees, or marketing arrangements with record labels.<sup>21</sup> Napster's most valuable product may ultimately turn out to be the data it could collect on consumers' musical tastes and listening habits, data which could then be sold to music marketers.<sup>22</sup>

Napster has taken the Internet by storm. As of early April 2000, there were over 5 million registered Napster users,<sup>23</sup> many of whom regularly transfer MP3 files onto their hard drives at no cost. News of Napster has spread by word of mouth, and as more people have gained access to the system, the number of MP3 files available through Napster has grown exponentially.<sup>24</sup> In November 1999, a person who connected to Napster could obtain anywhere from 60,000 to 100,000 MP3 files, depending on the number of users connected at that moment. By June 2000, the average number of available MP3 files had grown to about 600,000.<sup>25</sup> These MP3 files consist primarily of modern rock, but

---

18. See Telephone Interview with David Weekly, Computer Scientist at Stanford University (Mar. 12, 2000) [hereinafter Weekly Interview]. Some users decline to share their files with others in the apparently unfounded fear that outside entry would compromise the security of their system, even for the limited purpose of copying MP3 files; See Parker Interview, *supra* note 17. Others might be unwilling to share files because the process of uploading files to other users slows down the process of downloading files to one's own computer due to the consumption of bandwidth. *Id.*

19. See Cohen, *supra* note 14, at 41.

20. See Telephone Interview with Lyn Jensen, CFO, Napster, Inc. (Mar. 17, 2000) [hereinafter Jensen Interview].

21. See Parker Interview, *supra* note 16.

22. See Harmon, *supra* note 5.

23. See Mike Musgrove and Robert Thomason, *Napster Shares Files, Raises Ire*, WASH. POST, Apr. 7, 2000, at E1, available in 2000 WL 2295459.

24. See *id.*

25. See Parker Interview, *supra* note 16. Many of these files are duplicates—identical ones available from more than one Napster user. *Id.* For example, a search for Copeland's *Appalachian Spring* might yield 15 potential sources. One would then choose from whom to download based on the speed of the source's modem and the sound quality of his recording. However, the aforementioned 600,000 figure was from only one server of which there



files are also available in genres such as classical, opera, country, comedy, and anything else other Napster users are willing to share. Among college students, Napster has spread so quickly that "the resulting glut of digital traffic has overloaded university networks. Dozens of colleges, including New York University and the University of California at Berkeley, have banned students from using the service."<sup>26</sup> Indiana University blocked student access to Napster after it realized that Napster use was consuming nearly 60% of the available bandwidth.<sup>27</sup>

#### IV. RIAA'S LAWSUIT AGAINST NAPSTER

On December 9, 1999, eighteen music companies filed suit in the U.S. District Court for Northern California with the RIAA's assistance, alleging that Napster is engaging in contributory copyright infringement and is also vicariously liable for direct copyright infringement by its users.<sup>28</sup> The RIAA reasons:

Plaintiffs and their recording artists are compensated for their creative efforts and monetary investments largely from the sale of phonorecords to the public and from license fees from the reproduction, distribution, digital performance, or other exploitation of such phonorecords. Absent such compensation, profits and motivation are siphoned away from artists and the record companies that record, manufacture, promote, and distribute those works. The pool of resources available for finding and promoting new artists shrinks, and sound quality and recording integrity are diluted and corrupted. The ultimate result is that the public's access to a wide variety of high-quality musical recordings is sharply curtailed.<sup>29</sup>

Claiming that on average 90% of recordings available through Napster infringe copyrights held by its members' labels, the RIAA is seeking statutory damages of \$100,000 for each copyright-protected song exchanged using Napster.<sup>30</sup> The total amount of damages sought exceeds \$100 million and if awarded would put Napster out of business.<sup>31</sup>

---

are a total of 150. These servers are currently not connected and are assigned to users randomly during each session. However, there are plans for linking them, and once this occurs the number of files simultaneously available to an individual user will increase substantially. See <<http://www.napigator.com>>. A user can connect to a website that enables him to select a specific Napster server. *Id.*

26. See Harmon, *supra* note 5. See also David Weekly, *How to Access Napster When It's Blocked* (visited Apr. 27, 2000) <<http://www.david.weekly.org/code/napster-proxy.php3>> (noting that this blockage can easily be bypassed by selecting a proxy server).

27. See Amy Kover, *Who's Afraid of This Kid? The Recording Industry, That's Who.*, FORTUNE MAG., Mar. 20, 2000, at 129, available in 2000 WL 3461856.

28. A&M Records v. Napster, Inc., No. 99-5183 (N.D. Cal. filed Dec. 6, 1999).

29. *Id.* para. 30.

30. See Clark, *supra* note 2.

31. See *id.*

Though the exact amount of damages is debatable, there are indications that widespread use of Napster has the potential to reduce record sales.<sup>32</sup> A reporter quoted one young woman as saying “I love Napster. I’m never buying a CD again.”<sup>33</sup> In one of the more egregious examples of copyright infringement, Madonna’s remake of *American Pie* appeared on Napster several weeks before it was even released by the record companies, courtesy of someone who transferred (i.e., “ripped”)<sup>34</sup> a copy of an advance-promotion CD to his hard drive, and then made it available to other Napster users.<sup>35</sup> Sean “Puffy” Combs’ album, *Born Again*, was also available on Napster prior to its public release, infuriating Mr. Combs.<sup>36</sup>

## V. COPYRIGHT LAW IN THE DIGITAL AGE

### A. BACKGROUND

Copyright law was first developed in the late middle ages in response to the invention of the printing press.<sup>37</sup> Its goal has always been to balance society’s interest in access to information against the right of the information’s creators to profit from the fruits of their labor.<sup>38</sup> In this country, copyright law was established by Congress pursuant to Article I, Section 8 of the Constitution, which states that “Congress shall have power. . . [t]o promote the Progress of Science and useful Arts, by securing for limited Times to Authors and Inventors the exclusive Right to their respective Writings and Discoveries.”<sup>39</sup>

The statutory framework for copyright law is set out in 17 U.S.C. §§ 101-1101,<sup>40</sup> and gives a copyright holder the exclusive rights to reproduce, distribute, perform, prepare derivative works, and display the copyrighted work.<sup>41</sup> In simplified terms, “a copyright for a musical work created on or after January 1, 1978, subsists from its creation and . . . endures for a term consisting of the life of the author plus 70 years following the author’s death.”<sup>42</sup> Copyrights “subsisting on January 1, 1978 . . . endure for 28 years from the date [the copyright] was originally secured, [and can be renewed for a] further term of

---

32. See *Kover*, *supra* note 27, at 129.

33. See *id.*

34. See Harmon, *supra* notes 5, 13, at A1 and accompanying text.

35. See Cohen, *supra* note 14.

36. See Sherman Fridman, *Napster Operates a Pirate Bazaar - RIAA*, NEWSBYTES NEWS NETWORK, Dec. 10, 1999, available in 1999 WL 29943883.

37. See Kevin Davis, *Fair Use on the Internet: A Fine Line Between Fair and Foul*, 34 U.S.F. L. REV. 129, 132 (1999).

38. See *id.* at 132 n.14.

39. U.S. CONST. art. I, § 8, cl. 8.

40. See 17 U.S.C. §§ 101-1101 (2000).

41. See Davis, *supra* note 37, at 134; see also 17 U.S.C. § 106 (2000)

42. 17 U.S.C. § 302(a) (2000).

67 years.”<sup>43</sup>

“Copyright infringement occurs when an individual uses, or authorizes the use of, the copyrighted material [without prior permission and] in a way that trespasses into any of the copyright holder’s exclusive rights.”<sup>44</sup> “Copyright law imposes ‘absolute liability’ for [infringement, which means that] the copyright owner can [obtain] both injunctive relief . . . and monetary damages . . . whether the person violating the rights did so intentionally or by accident.”<sup>45</sup> It is the copyright owner’s burden to prove copyright infringement.<sup>46</sup>

## B. BASIC FORMS OF COPYRIGHT INFRINGEMENT

### 1. *Direct Liability*

An individual is directly liable for copyright infringement if he has copied material protected by a valid copyright.<sup>47</sup> It is the copyright owner’s burden to prove this, though he does not need to prove the defendant’s intent or knowledge of the infringement.<sup>48</sup> However, there are two major exceptions to direct copyright infringement, the common law Fair Use Doctrine and the Audio Home Recording Act (“AHRA”).

Under the Fair Use Doctrine, a defendant may escape liability if he can prove that his use was reasonable based on: (1) the purpose and character of the use (i.e., the more commercial it is, the less fair);<sup>49</sup> (2) the nature of the copyrighted work (i.e., the more creative it is and the less informational, the less fair);<sup>50</sup> (3) the amount and substantiality of the portion used;<sup>51</sup> and (4) the effect of unrestricted and widespread conduct of the sort engaged in by the defendant on the plaintiff’s potential market for the work.<sup>52</sup> All of these factors must be considered, with

43. See *id.* § 304(a)(1)-(2).

44. See Davis, *supra* note 37, at 134-35.

45. See Mark Radcliffe, *Digital Millennium Copyright Act Forging the Copyright Framework for the Internet: First Steps*, PRAC. L. INST., 557 PLI/Pat 365, 370 (1999).

46. See Jennifer E. Markiewicz, *Seeking Shelter from the MP3 Storm: How Far Does the Digital Millennium Copyright Act Online Service Provider Liability Limitation Reach?*, 7 COMM. LAW CONSPICUOUS 423, 427 (1999).

47. See Donna M. Lampert et al., *Overview of Internet Legal and Regulatory Issues*, PRAC. L. INST., 544 PLI/Pat 179, 223 (1998).

48. See Markiewicz, *supra* note 46, at 427.

49. See *American Geophysical Union v. Texaco, Inc.*, 802 F. Supp. 1, 24 (S.D.N.Y. 1992), *aff’d*, 60 F.3d 913 (2d Cir. 1994), *cert. dismissed*, 516 U.S. 1005 (1995).

50. See *Harper & Row Publishers v. Nation Enterprises*, 471 U.S. 539, 563 (1985); see also 17 U.S.C. § 107 (2000).

51. See *Sony Corp. of Am. v. Universal City Studios*, 464 U.S. 417, 450 n.30 (1984) (copying an entire work ordinarily militates against a finding of fair use). *Id.* at 449-50; see also 17 U.S.C. § 107 (2000).

52. See *Campbell v. Acuff-Rose Music*, 510 U.S. 569, 590 (1994); see 17 U.S.C. § 107 (2000).

the fourth given the most weight.<sup>53</sup>

Congress's passage in 1992 of the AHRA lent more definition to the Fair Use Doctrine.<sup>54</sup> Under the AHRA, no lawsuit may be brought "alleging infringement of copyright based on the . . . noncommercial use by a consumer of [a digital audio recording device or medium] for making digital or analog musical recordings."<sup>55</sup> This resolved the prior uncertainty regarding the legal ramifications of home taping.<sup>56</sup>

## 2. *Contributory Liability*

Contributory copyright liability "originates in tort law and stems from the notion that one who directly contributes to another's infringement should be held accountable."<sup>57</sup> A party is contributorily liable, and thus subject to monetary<sup>58</sup> damages and injunctive<sup>59</sup> relief,<sup>60</sup> if it has knowledge (or reason to know) of the infringing conduct of another, and induced, caused, or materially contributed to this conduct.<sup>61</sup> Participation by the defendant need not be "substantial."<sup>62</sup>

"Contributory infringement . . . is of two types – personal conduct that forms part of or furthers the infringement and contribution of machinery or goods that provide the means to infringe."<sup>63</sup> In the absence of a physical product that is the subject of the alleged infringement, "the extent of control exercised by the defendant over the third party's means of infringement" is considered.<sup>64</sup> The greater the degree of control, the greater the likelihood that contributory infringement will be found.

In *Fonovisa v. Cherry Auction, Inc.*, swap meet operators were held contributorily liable for the infringing activities of vendors who were selling copyrighted music recordings without permission.<sup>65</sup> The direct liability of the operators having been established, the court needed to determine whether the operators' participation level was enough to war-

---

53. See *Sega Enters. Ltd. v. MAPHIA*, 948 F. Supp. 923, 935 (N.D. Cal. 1996).

54. 17 U.S.C. § 1008 (2000).

55. See *id.*

56. See John W. Hazard, Jr., COPYRIGHT LAW IN BUSINESS AND PRACTICE § 8.03, n.269 (Rev. ed. 1999).

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

58. David Nimmer, NIMMER ON COPYRIGHT § 14.02(A) 14-8, (1999), available in LEXIS (Copyright Law, Treatises & Analytical Materials, Matthew-Bender).

59. See *id.* at § 14.06(C) 14-123.

60. See Markiewicz, *supra* note 46, at 433; see also 17 U.S.C. §§ 502–505 (2000).

61. See *Gershwin Publishing Corp. v. Columbia Artists Management*, 443 F.2d 1159, 1162 (2d Cir. 1971).

62. See *Fonovisa*, 76 F.3d at 264.

63. See Nimmer, *supra* note 58, § 12.04(A)(2).

64. *Lockheed Martin v. Network Solutions*, 194 F.3d 980, 984 (9th Cir. 1999)

65. See *Fonovisa*, 76 F.3d at 259, 264 (1996).

rant contributory infringement.<sup>66</sup> According to the Ninth Circuit, providing the site and facilities where the provider knew infringing activity was occurring was sufficient to create contributory liability.<sup>67</sup> Though this case did not involve the Internet, it has influenced the legal analysis of contributory liability in cyberspace.<sup>68</sup>

### 3. *Vicarious Liability*

A party is vicariously liable for copyright infringement when it has the authority to supervise a direct infringer's actions; has induced, caused, or materially contributed to the infringing activity;<sup>69</sup> and has a direct financial benefit from the infringing activity.<sup>70</sup> Unlike contributory infringement, vicarious liability may be imposed even if a defendant has no direct knowledge of the infringing activity. Courts developed the concept of vicarious liability in an effort to "fashion a principle for enforcing copyrights against a defendant whose economic interests were intertwined with the direct infringer's, but who did not actually employ the direct infringer."<sup>71</sup> As with contributory infringement, remedies for vicarious liability include both monetary damages and injunctive relief.<sup>72</sup>

An example of someone who would be held vicariously liable is a nightclub owner who sells more tickets when a band illegally performs copyrighted music in his nightclub. "If the band has fail[ed] to obtain a public performance license for" the songs it plays, it is liable for direct infringement of the music composition owner's copyright.<sup>73</sup> The nightclub owner, in turn, is vicariously liable because he benefits financially through increased attendance at his nightclub because he has the ability to control the band.<sup>74</sup>

Another example of vicarious liability is what was done by Cherry Auction. The *Fonovisa* court found Cherry Auction to be vicariously liable in addition to having engaged in contributory infringement because it "promoted the swap meet and controlled the access of customers to the swap meet area."<sup>75</sup> Furthermore, Cherry Auction derived "substantial financial benefits from admission fees, concession stand sales and park-

66. *See id.*

67. *See id.*

68. *See* Timothy L. Skelton, *Internet Copyright Infringement and Service Providers: The Case for a Negotiated Rulemaking Alternative*, 35 SAN DIEGO L.REV. 219, 252 (1998).

69. *See* Markiewicz, *supra* note 46, at 427.

70. *See id.*

71. *Fonovisa*, 76 F.3d at 262 (discussing the landmark vicarious liability case of *Shapiro, Bernstein and Co. v. H.L. Green Co.*, 316 F.2d 304 (2d Cir. 1963)).

72. *See* Markiewicz, *supra* note 46, at 433; *see generally* Nimmer, *supra* note 59, § 12.04(A)(2).

73. *See* Radcliffe, *supra* note 45, at 371.

74. *See id.*

75. *See Fonovisa*, 76 F.3d at 262.

ing fees, all of which flow directly from customers who want to buy the counterfeit recordings at bargain basement prices.”<sup>76</sup>

C. ONLINE COPYRIGHT INFRINGEMENT LIABILITY LIMITATION ACT  
(TITLE II)

Continued expansion of the Internet brought ISPs increasingly into conflict with copyright holders. Unless copyright law was modernized, growth of the Internet would be hampered because ISPs could not constantly police the huge amount of information that is stored or passes through their networks. In response to this situation, in 1998 Congress passed the Online Copyright Infringement Liability Limitation Act, which was incorporated as Title II of the Digital Millennium Copyright Act (DMCA).<sup>77</sup> David Nimmer has written that “. . .by limiting the liability of service providers, the DMCA ensures that the efficiency of the Internet will continue to improve and that the variety and quality of services on the Internet will continue to expand.”<sup>78</sup>

Title II retains the traditional elements required to prove copyright infringement.<sup>79</sup> However, an ISP found to be contributorily or vicariously liable for copyright infringement can avoid monetary penalties<sup>80</sup> and will not have its operations shut down<sup>81</sup> if it can prove that its activities are protected under Title II.<sup>82</sup> The only penalty that can be imposed on such an ISP is a narrow injunction to block access to individual infringing users.<sup>83</sup> As noted in Napster’s *Motion for Summary Adjudication*, “[t]his is consistent with the DMCA’s allocation of responsibilities to individual users not to infringe. . .”<sup>84</sup> In determining whether or not to impose an injunction, the court must weigh the financial burden of the ISP against the harm suffered by the copyright owner if no action is taken to remove the infringing material or activity.<sup>85</sup> An ISP proves that it merits Title II limited liability protection by demonstrating that it is, in fact, an ISP as defined by the statute, and also that it engages in at least one of four protected functions.

---

76. *Id.* at 263.

77. See Markiewicz, *supra* note 46, at 424. See also Radcliffe, *supra* note 45, at 367. The DMCA, Pub. L. No. 105-304, was signed into law on October 28, 1998.

78. See Nimmer, *supra* note 58, at § 12B.01 C1.

79. See Markiewicz, *supra* note 46, at 424.

80. See Radcliffe, *supra* note 45, at 373.

81. See *Def. Napster, Inc.’s Notice of Mot. and Mot. for Summ. Adj.; Mem. of P. & A. in Supp. Thereof* (N.D. Cal. 2000) (No. C99-5183), at 22 [hereinafter *Napster’s Mot. for Summ. Adj.*].

82. See H.R. REP. NO. 105-551, pt. 1 (1998), available in 1998 WL 261605, at \*67.

83. See 17 U.S.C. § 512(j)(1)(B) (2000).

84. *Napster’s Mot. for Summ. Adj.*, *supra* note 81, at 22.

85. See 17 U.S.C. § 512(j)(2)(A)-(D) (2000).

### 1. *Title II Internet Service Provider Status*

As a practical matter, any Internet-based entity that facilitates access to the Internet and its various resources is considered an ISP.<sup>86</sup> More formally, an ISP is any entity that transmits, routes, or provides "connections for digital online communications, between or among points specified by a user, of material of the user's choosing, without modifying the content of the material as sent or received."<sup>87</sup> An entity that provides online services or network access would be considered an ISP if it temporarily stores information on its servers (System Caching), allows users to store information on its servers (User Storage), or provides links to information (Information Location Tool).<sup>88</sup>

### 2. *Title II Functional Safe Harbors*

#### a. *Transitory Digital Network Communications (Conduit)*

Limited liability is granted to ISPs that route or provide connections for information through their system and which is stored there only for as long as it takes to route the information to its next destination. Additional requirements are:

- (1) the transmission of the material is initiated by or at the direction of a person other than the ISP;
- (2) the ISP does not select the information and the routing and storage processes are automatic;
- (3) the ISP does not select the recipients of the material except as an automatic response to the request of another person;
- (4) any copies of the material made by the ISP during the course of any transient storage are accessible only to the anticipated recipients and are maintained on the ISP's system only for as long as is necessary to complete the transmission; and
- (5) the information is transmitted through the ISP's system without modification.<sup>89</sup>

Congress refers to transitory digital communications networks meeting these requirements as "conduits."<sup>90</sup>

#### b. *System Caching*

Limited liability is granted to ISPs that temporarily store material on their servers in order to provide quick and easy access by their users.<sup>91</sup> Information is sometimes briefly stored on an ISP's system in order to "facilitate access by users subsequent to the one who previously sought access to it."<sup>92</sup> In order to qualify for this form of limited liability, ISPs

---

86. See Radcliffe, *supra* note 45, at 376.

87. 17 U.S.C. § 512(k)(1)(A)(2000).

88. 17 U.S.C. § 512(k)(1)(B).

89. 17 U.S.C. § 512(a)(1)-(5).

90. H.R. REP. No. 105-551, pt. 2 (1998), available in 1998 WL 414916, at \*131.

91. 17 U.S.C. § 512(b)(1)-(2) (2000).

92. H.R. REP. No. 105-551, pt. 2 (1998), available in 1998 WL 414916, at \*131.

providing System Caching must subject their users to the same conditions of access (e.g., fees, passwords) as the originating site would have imposed.<sup>93</sup>

*c. Information Residing on Systems at Direction of Users (User Storage)*

Limited liability is granted to an ISP that stores copyright infringing material on its system at the behest of a third party, as long as the ISP

- (1) does not have actual knowledge or awareness that the material is infringing;
- (2) upon obtaining such knowledge or awareness acts expeditiously to remove, or disable access to, the information;
- (3) does not receive a financial benefit directly attributable to the infringing activity;
- and (4) upon receiving notification of the infringing activity or information, responds expeditiously to remove or disable access to the relevant material.<sup>94</sup>

In order to qualify for this status, the ISP must also have a Designated Agent to receive notifications of alleged infringements.<sup>95</sup>

*d. Linking to Infringing Material Via Information Location Tools*

Information location tools are essential to the operation of the Internet because without them, users would not be able to find the information they need.<sup>96</sup> In an effort to promote their development, a limited liability safe harbor was thus created for ISPs that link users to online locations through directories, indexes, references, pointers, or hypertext links.<sup>97</sup>

Limited liability is granted even if the online locations contain infringing material or activity, as long as the ISP

- (1) does not have actual knowledge of infringement at the other online location nor awareness of facts and circumstances from which infringing activity in that location is apparent; and
- (2) upon obtaining such knowledge or awareness, acts expeditiously to remove, or disable access to, the material.<sup>98</sup> [Furthermore, the ISP must not] (1) receive a financial benefit directly attributable to the infringing activity, in a case in which the ISP has the right and ability to control such activity, and (2) upon notification of claimed infringement to a Designated Copyright Agent, [must respond] expeditiously to remove or disable access to the material that is claimed to be infringing or to be the subject of infringing-

---

93. 17 U.S.C. § 512(b)(1)-(2) (2000).

94. 17 U.S.C. § 512(c)(1).

95. 17 U.S.C. § 512(c)(2).

96. See Nimmer, *supra* note 58, at § 12B.05, A1.

97. See Jeffrey P. Cunard et al., *Internet Law*, PRAC. L. INST., 581 PLI/Pat 853, 870 (1999).

98. 17 U.S.C. § 512(d)(1)(C) (2000).



ing activity.<sup>99</sup>

This portion of the statute is vague with regard to the knowledge component. On the one hand, an ISP engaged in information location has no obligation to proactively seek out copyright infringement by its users.<sup>100</sup> Title II states that an ISP is not required to engage in “monitoring its service or affirmatively seeking facts indicating infringing activity. . .” in order to obtain safe harbor protection.<sup>101</sup> Furthermore, an ISP will not lose liability protection if it becomes aware of material that is only “suspect,” and not “obvious[ly]” infringing.<sup>102</sup> On the other hand, the analysis provided by the House Committee on the Judiciary states that an ISP will not qualify for liability limitation if it ignores “red flags” of blatant infringement.<sup>103</sup> It is unclear how blatant the infringement must be before the ISP is held to be ignoring a “red flag.”

## VI. NAPSTER'S LEGAL LIABILITY

### A. DIRECT COPYRIGHT INFRINGEMENT BY NAPSTER'S USERS

Arguments can be made on both sides of the issue of whether Napster's users are engaging in direct copyright infringement when they download or share copyrighted music. Many Napster supporters believe that enough elements of the Fair Use defense exist to exempt Napster users from direct liability. They argue that the use of Napster is not commercial because Napster users, typically young people on a budget, would not buy the songs in a record store anyway. With no economic loss to the record companies, the use of Napster cannot be considered commercial. Others argue that using Napster to download MP3 files actually helps the music industry by stimulating the purchase of CDs, the result of people having had the opportunity to sample artists with whom they might not otherwise be familiar. This argument is supported by the fact that “in 1999, the first year in which MP3 technology was widely available, the record industry experienced 8% growth in revenue. . . .”<sup>104</sup>

For the purposes of assessing Napster's contributory and vicarious liability, this paper will assume that those who use Napster to transfer copyrighted music files *are* engaging in direct copyright infringement. Such users would not be able to invoke the Fair Use Doctrine as a defense because under the four-step analysis discussed above, (1) Napster

---

99. 17 U.S.C. § 512(d)(2)-(3).

100. See Markiewicz, *supra* note 46, at 438.

101. 17 U.S.C. § 512(m)(1) (2000).

102. See Markiewicz, *supra* note 46, at 438.

103. See *id.*

104. Brian Ploskina, *Record Industry Shoots Itself with MP3 Bullet*, INTERACTIVE WEEK FROM ZDWIRE, Apr. 17, 2000, available in 2000 WL 4065877 (citing statistics provided by the RIAA).

users typically download MP3 files to avoid paying for them in record stores<sup>105</sup> and are rarely just making a backup copy or copying a single song for a friend; (2) the copyrighted works are for uses that are more creative than informational, which weighs against a finding of fair use;<sup>106</sup> (3) the entire copyrighted music files are typically downloaded to users' hard drives; and (4) the effect on the music industry is to reduce the potential market for the work.<sup>107</sup>

Many readers will be relieved to learn that the RIAA has stated that it does not plan to prosecute Napster users for direct copyright infringement,<sup>108</sup> which is a federal crime punishable by up to three years in prison and \$250,000 in fines.<sup>109</sup> The RIAA recognizes that such a move could induce retaliatory consumer boycotts of legitimate music purchases, and as such would not be a good marketing strategy. Nevertheless, given that the direct infringement exists, the RIAA is still able to press a claim against those it alleges to be contributorily and vicariously liable.

#### B. ASSESSMENT OF NAPSTER'S CONTRIBUTORY LIABILITY

The RIAA has accused Napster of contributory copyright infringement, and will therefore need to show that Napster knowingly induces, causes, or materially contributes to infringing activities by its users. It is unlikely that the RIAA will be able to demonstrate that Napster induced or caused copyright infringement. The terms "induce" and "cause" indicate the defendant's initiation of infringing activity, yet Napster is a passive system that merely responds to its users' queries. Users, not Napster, initiate the transfer of MP3 files. Furthermore, Napster does nothing to encourage its users to make even non-copyrighted MP3 files available for uploading, let alone copyrighted ones. As previously mentioned, a user can download files even if he is not willing to share his own files with others.

It will be harder for Napster to refute allegations that it materially contributed to copyright infringement by some of its users. Though the term "material contribution" has not yet been defined by courts in the online context, it can plausibly be argued that without Napster, people would find it much more difficult to locate and download copyrighted ma-

---

105. See *American Geophysical Union v. Texaco, Inc.*, 802 F. Supp. 1, 14-16 (S.D.N.Y. 1992), *aff'd*, 60 F.3d 913 (2d Cir. 1994), *cert. dismissed*, 516 U.S. 1005 (1995). No fair use was found where scientists photocopied publication in order to avoid cost of purchasing additional copies from publisher. *Id.*

106. See *Harper & Row Publishers v. Nation Enters.*, 471 U.S. 539, 563 (1985).

107. 17 U.S.C. § 107 (2000).

108. See Harmon, *supra* note 5, at A1.

109. See Chad Swiatecki, *Michigan State U.: Stiff Fines, Jail Not Detering Napster Users*, U-WIRE, Apr. 14, 2000, available in 2000 WL 19350225.

terial. By this reasoning, Napster greatly facilitates, and therefore materially contributes to, copyright infringing activity.

Even if the RIAA can convince the court that Napster materially contributes to its users' infringing activity, it will be difficult to prove that Napster had knowledge of this infringing activity. First, ISPs are under no affirmative obligation to seek out copyright infringing activity on their systems.<sup>110</sup> Second, Napster has much less reason to be aware of the activities of its registrants than did Cherry Auction, the swap meet operator in *Fonovisa*. Whereas the swap meet operator and its registrants shared the same physical space, Napster and its registrants have no physical contact following the initial registration, though they do have a minimal degree of contact in cyberspace.<sup>111</sup> Third, knowledge of infringing activity cannot be presumed where a legitimate use for a device or system exists. Several reported decisions involving similar facts support this conclusion.

In *Sony v. Universal*, 464 U.S. 417 (1984), the movie industry tried to prevent the Sony Corporation from selling its Betamax Video Cassette Recorder (VCR) on the grounds that it had constructive knowledge that the VCR was being used to make illegal copies of copyrighted films.<sup>112</sup> Ruling in favor of Sony, the Court stated 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. Indeed, it need merely be capable of substantial noninfringing uses"<sup>113</sup> such as time-shifting (recording a television program for later viewing). As with the VCR, Napster is capable of being used for the legitimate purpose of listening to and sharing non-copyrighted material, which the RIAA itself acknowledges exists on the Internet.<sup>114</sup>

The District Court for the Central District of California was faced with a situation similar to *Sony* in 1998, when the RIAA sought an injunction against Diamond Multimedia to stop impending distribution of its Rio PMP 300 ("Rio").<sup>115</sup> The Rio is a handheld device that can receive MP3 files from a computer's hard drive, store up to two hours of music,

---

110. See 17 U.S.C. § 512(m) (2000) ("Nothing in this section shall be construed to condition the applicability of subsections (a) through (d) on . . . (1) a service provider monitoring its service or affirmatively seeking facts indicating infringing activity. . .").

111. This applies the reasoning used in *Academy of Motion Picture Arts and Sciences v. Network Solutions*, 45 U.S.P.Q. 2d 1463, 1467 (C.D. Cal. 1997), available in 1997 WL 829341.

112. See *Sony Corp. of Am. v. Universal City Studios*, 464 U.S. 417 (1984).

113. *Id.* at 442.

114. See *A&M Records v. Napster, Inc.*, No. 99-5183 (N.D. Cal. filed Dec. 6, 1999), at para. 43.

115. See *Recording Indus. Assoc. of Am. v. Diamond Multimedia Sys.*, 29 F. Supp. 2d 624, at 635 (C.D. Cal. 1998), *aff'd*, 180 F.3d 1072 (9th Cir. 1999).

and then play this music back.<sup>116</sup> As such, this device functions as a “space-shifter” in that one can listen to music while away from one’s computer. The RIAA argued that the Rio can be used to make serial digital copies of music (i.e., copies of copies) because although it does not have digital audio output capability, its memory card can be transferred to any other Rio.<sup>117</sup> As such, the Rio should be considered a recording device,<sup>118</sup> which is defined by the AHRA to be:

... 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.<sup>119</sup>

As a recording device, the Rio would be subject to the AHRA’s stringent provisions for such devices. This would require Diamond to make a 2% royalty payment on sales to the Register of Copyrights at the Library of Congress, for ultimate redistribution to the appropriate copyright holders.<sup>120</sup> More importantly, Diamond would have to modify the Rio by adding Serial Copy Management System (SCMS) technology to prevent it from making serial digital copies.<sup>121</sup>

The court held that although the Rio is capable of serial copying, the AHRA does not directly prohibit such copying.<sup>122</sup> In any event, “because the Rio itself has no digital output capability, and the removable flash memory cards cannot be copied by another Rio device,” the Rio adequately prohibits unauthorized serial copying and is not subject to the additional burden of having to incorporate SCMS technology.<sup>123</sup> Finally, the court stated that even if the Rio were considered a recording device, no injunction could have been issued against it because it can be used to record “legitimate music” and is “a device with significant beneficial uses.”<sup>124</sup> This last point is directly applicable to Napster, which can be used for the legitimate purpose of sharing non-copyrighted music.

---

116. *See id.*

117. *See id.*

118. *See* Dibbell, *supra* note 10 at 106.

119. *See* 17 U.S.C. § 1001(3) (2000).

120. *See* Dibbell, *supra* note 10; *see also* 17 U.S.C. § 1003(a) (2000); *see also* 17 U.S.C. § 1004(a)(1) (2000).

121. *See* Dibbell, *supra* note 10. *See also* Hazard, *supra* note 56. SCMS encodes digital information onto any first-generation copy of a digital musical recording (digital information not contained in the factory original). *Id.* The newly encoded information distinguishes between the factory original and the subsequently created first-generation copy in order to prohibit future digital copying from that first-generation copy, while continuing to permit unlimited copying from the factory original. *Id.*

122. *See Recording Indus. Assoc. of Am.*, 29 F. Supp. 2d at 631.

123. *See id.* at 632.

124. *See id.* at 633.

The final consideration when dealing with an allegation of contributory liability in the absence of a physical product is "the extent of control exercised by the defendant over the third party's means of infringement."<sup>125</sup> In *Fonovisa*, the court viewed Cherry Auction as having "direct control over the activity that the third-party alleged infringers engaged in on the premises" because it had licensed real estate to those alleged infringers.<sup>126</sup> Renting space, even at a flea market, creates a legal duty by the landlord to control illegal activities on his premises.<sup>127</sup> Napster, on the other hand, bears more similarity to the defendant in *Lockheed Martin v. Network Solutions*, 194 F.3d 980 (9th Cir. 1999). In that case, the court held that Network Solutions, a provider of Internet domain names, had little control over potential copyright infringers given that its function was more akin to the Postal Service "performing the routine service of routing mail."<sup>128</sup>

### C. ASSESSMENT OF NAPSTER'S VICARIOUS LIABILITY

Napster would be vicariously liable if it has the authority to supervise its users' actions; induces, causes, or materially contributes to infringing activity by its users;<sup>129</sup> and has a direct financial benefit from its users' infringing activity.<sup>130</sup> Napster would not need to have direct knowledge of directly infringing activity by its users in order to be held vicariously liable.

Napster does not supervise its users' actions after they obtain the initial linking information from Napster's servers. MP3 file transfers occur directly from user to user with no involvement by Napster. Indeed, Napster only controls its users' access to its system if it wants to *remove* them for engaging in copyright infringing activity. This stands in contrast to Cherry Auction, which actively controlled access of its customers to the swap meet area.<sup>131</sup> Though Napster used to provide an "Auto Resume" feature by which its system would automatically transmit new links to help complete any interrupted MP3 downloads, the company terminated this service in January 2000.<sup>132</sup>

As discussed above, Napster is a passive system that reacts to its users' queries and therefore does not induce or cause its users to violate

---

125. *Lockheed Martin v. Network Solutions*, 194 F.3d 980, 984 (9th Cir. 1999).

126. *Id.* at 985 (citing *Fonovisa v. Cherry Auction, Inc.*, 76 F.3d 259, 265 (9th Cir. 1996)).

127. *See id.* at 984 (citing *Hard Rock Cafe Licensing v. Concession Servs.*, 955 F.2d 1143, 1149 (7th Cir. 1992)).

128. *Id.*

129. *See Markiewicz, supra* note 46, at 427.

130. *Id.*

131. *See Fonovisa*, 76 F.3d at 262.

132. *Pl.'s Opp'n to Napster's Mot. for Summ. Adj.*, *supra* note 15, at 13.

copyright laws. Unlike Cherry Auction, Napster does not promote its service through advertising. Napster users learn about the service through word of mouth or by reading about it in the press.

Napster would probably have to concede that it has materially contributed to direct copyright infringement by its users. Without Napster, people would find it much more difficult to locate and download copyrighted material. Napster greatly facilitates, and thereby materially contributes, to copyright infringing activity.

It is unlikely that the Ninth Circuit will determine that Napster receives a direct financial benefit from any infringing activity by its users. Courts have dismissed “[t]heories alleging that infringing activity enhances the value of an ISP’s service, thus attracting more subscribers. . .”<sup>133</sup> Napster does not presently charge an admission fee from its users or receive advertising revenue, and is instead financed solely from venture capital.<sup>134</sup> Even if it did charge an admission fee or obtain advertising revenue, it is unlikely that the RIAA could prove that the value of Napster’s service “lies in providing access to infringing material,”<sup>135</sup> given that Napster is highly useful even when used solely for the purpose of sharing non-copyrighted material. Furthermore, courts have held that fixed fees in the online context negate any direct financial benefit from alleged infringement.<sup>136</sup>

Applying the various tests to assess vicarious liability, on balance it appears that Napster cannot be held vicariously liable for any directly infringing activity by its users. Though it is reasonable to conclude that Napster materially contributes to those who decide to violate copyright laws, Napster does not supervise its users’ activities, nor does it induce or cause them to engage in copyright violations. Furthermore, Napster does not receive a direct financial benefit from any infringing activity by its users.

#### D. NAPSTER’S PROTECTED STATUS UNDER TITLE II

Under the preceding analysis, Napster should not be held contributorily or vicariously liable for copyright infringement by its users. However, in the event that the reviewing court decides otherwise, it would then have to determine if Napster is exempted from liability because it is an ISP engaged in a protected function.

---

133. See Markiewicz, *supra* note 46, at 433.

134. See Parker Interview, *supra* note 16.

135. H.R. REP. NO. 105-551, pt. 1 (1998), available in 1998 WL 261605, at \*66.

136. See, e.g., Religious Technology Ctr. v. Netcom On-Line Comm. Servs., 923 F. Supp. 1231, 1376-77 (N.D. Cal. 1995).

### 1. *Napster's Internet Service Provider Status*

Napster is an ISP as defined in § 512(k)(1)(A) because it offers the "transmission, routing, or providing of connections for digital online communications" and "provid[es] connections for digital online communications, between or among points specified by a user, of material of the user's choosing, without modifying the content of the material as sent or received."<sup>137</sup> Napster's system is comprised of 150 computer servers to which Napster's users connect, proprietary MusicShare software that users install on their computers, and proprietary software that Napster runs on its own servers to control the process. The RIAA acknowledges that "[t]hese components work in unison to form a fully integrated online service."<sup>138</sup>

### 2. *Napster's Protected Function Status*

#### a. *Napster as a Transitory Digital Communications Network*

Napster argues that it should be classified as a § 512(a) Transitory Digital Communications Network.<sup>139</sup> It may have chosen this category because this would shield the company from a finding that it has knowledge of the infringing activity of its users.<sup>140</sup> Napster argues that it falls under § 512(a) because it merely routes information through its servers, stores the information there only for as long as its users are online, and meets the five-part test outlined in § 512(a)(1)-(5).<sup>141</sup> First, Napster points out that the transmission of the Internet linking information is initiated solely at the direction of a person *other* than Napster, satisfying § 512(a)(1).<sup>142</sup> Second, Napster maintains that it satisfies § 512(a)(2) because it does not select information to be transmitted.<sup>143</sup> Congress has explained that the selection of information is demonstrated by exercising editorial control in determining what material to send, something which Napster does not do.<sup>144</sup> Furthermore, Napster's routing and storage processes are automatic because its users are the ones who determine what information they wish to share and download, as well as when this is to occur.<sup>145</sup> Third, Napster argues that it does not select the recipients of the material, who select themselves, and that it therefore meets

---

137. 17 U.S.C. § 512(k)(1)(A) (2000).

138. See *Pl.'s Opp'n to Napster's Mot. for Summ. Adj.*, *supra* note 15, at 8.

139. See *Def. Napster, Inc.'s Reply Mem. of P. & A. in Supp. of Mot. for Summ. Adj.* (N.D. Cal. 2000) (No. C99-5183).

140. See Telephone Interview with Stanley Pierre-Louis, Attorney, Napster, Inc. (Apr. 7, 2000) [hereinafter Pierre-Louis Interview].

141. See *Napster's Mot. for Summ. Adj.*, *supra* note 81.

142. See *id.* at 11.

143. See *id.* at 12.

144. See H.R. REP. NO. 105-551, pt. 2 (1998), available in 1998 WL 414916, at \*131.

145. See *Napster's Mot. for Summ. Adj.*, *supra* note 81, at 12.

§ 512(a)(3).<sup>146</sup> Napster points out that the fourth and fifth requirements are inapplicable to it. The fourth requirement, § 512(a)(4), is inapplicable because at no time are any copies of MP3 files stored or copied by Napster's servers, given that "[a]ll files transfer directly from the computer of one Napster user to the computer of the requesting user."<sup>147</sup> The fifth requirement, § 512(a)(5), is met because Napster does not modify any information passing through its servers.<sup>148</sup>

The difficulty with classifying Napster under § 512(a) is that it is not clear that Congress contemplated this provision to apply to systems that route information links, and not the underlying information to which these links refer. Congress referred to Transitory Digital Communications Networks as "conduits," suggesting that they route underlying information through their servers and not just links to this information.<sup>149</sup> However, the statute itself vaguely refers to the transmission of "material," without further elaboration.<sup>150</sup>

As shall be seen, the RIAA believes that classification under the more stringent § 512(d) Information Location Tool category is warranted, arguing that "Napster's entire motion is based on the flawed premise that it can invoke the protections of 512(a) for *all* of its myriad functions, as long as it can fit *any* of those functions into the narrow safe harbor provided by 512(a)."<sup>151</sup> The RIAA points out that prior to the lawsuit, the Napster website described the system as "a free information location tool and integrated browser and communications service. . ."<sup>152</sup>

#### *b. Napster as a Provider of System Caching*

Napster is not a provider of system caching because it does not temporarily store user material on its servers. Only the titles of MP3s are stored on Napster's servers. Both sides to the dispute agree that this category does not apply to Napster.<sup>153</sup>

#### *c. Napster as a Provider of User Storage*

Napster does not store information for its users on its servers, and therefore does not qualify for this type of protected status. Again, both sides to the dispute agree that this category does not apply to

---

146. *See id.*

147. *Id.* at 13.

148. *See id.*

149. *See* H.R. REP. NO. 105-551, pt. 2 (1998), available in 1998 WL 414916, at \*131.

150. *See* 17 U.S.C. § 512(a) (2000).

151. *Pl.'s Opp'n to Napster's Mot. for Summ. Adj.*, *supra* note 15, at 1.

152. *Id.* at 3. Napster has since removed this statement from its website. *Id.*

153. *See Pl.'s Opp'n to Napster's Mot. for Summ. Adj.*, *supra* note 15; *Napster's Mot. for Summ. Adj.*, *supra* note 81.



Napster.<sup>154</sup>

*d. Napster as an Information Location Tool*

Napster has chosen not to characterize itself as an Information Location Tool, though a strong argument can be made that this category aptly describes its function given that it provides users seeking specific MP3 files with the IP addresses of willing hosts. The RIAA argues that Napster should fall under this category.<sup>155</sup> If Napster were characterized as an Information Location Tool, it would receive limited liability under Title II only if it:

- (i) does not have actual knowledge or awareness that the material or activity is infringing;<sup>156</sup>
- (ii) upon obtaining such knowledge or awareness, acts expeditiously to remove, or disable access to, the material.<sup>157</sup>
- (iii) does not receive a financial benefit directly attributable to the infringing activity, in a case in which the ISP has the right and ability to control such activity;<sup>158</sup> and
- (iv) upon notification of claimed infringement, responds expeditiously to remove, or disable access to, the material that is claimed to be infringing or to be the subject of infringing activity.<sup>159</sup>

*(i) Knowledge of Copyright Infringement*

Napster may have chosen not to classify itself as an Information Location Tool out of concern that it might have difficulty disputing allegations of its knowledge of infringing activity.<sup>160</sup> It is a paradox of Title II that an Information Location Tool ISP that only transmits links through its servers must satisfy this additional test, whereas a Transitory Digital Network ISP that functions as a conduit for any information whatsoever does not need to satisfy this test. The statute, as written, creates the strong incentive for an ISP that could categorize itself as either an Information Location Tool or a Transitory Digital Network to categorize itself as the latter in order to avoid the knowledge prong of the four-part test.

Proceeding under the assumption that Napster is an Information Location Tool, the RIAA states in its complaint that Napster is “well aware [that] virtually all of the reproductions and distributions it enables and encourages are infringing and in violation of federal copyright

154. *See id.*

155. *Id.* at 1.

156. 17 U.S.C. § 512(d)(1) (2000).

157. 17 U.S.C. § 512(d)(1).

158. 17 U.S.C. § 512(d)(2)-(3).

159. 17 U.S.C. § 512(d)(2)-(3).

160. *See Pierre-Louis Interview, supra* note 140.

and state laws.”<sup>161</sup> Even if Napster’s awareness could not be conclusively proved, the RIAA could have argued that sufficient “red flags” are available to give Napster constructive knowledge that infringing activity is taking place with its assistance, thereby disqualifying it from limited liability under the Information Location Tool exception. In support of this argument, the RIAA could have quoted the House Judiciary Committee’s definition of a “red flag” as including “information of any kind that a reasonable person would rely upon.”<sup>162</sup>

Close analysis of Title II and the *House Commerce Committee Section-By-Section Analysis of H.R. 2281* [*Commerce Committee Analysis*] does not provide a clear-cut answer, but leans towards the conclusion that Napster cannot be deemed to have actual or constructive knowledge of the potentially copyright-infringing activity of some of its users. The *Commerce Committee Analysis* gives as an example of a red flag a situation in which a copyright owner could prove that “. . .the provider was aware of facts from which infringing activity was apparent if the copyright owner could prove that the location was clearly, at the time the directory provider viewed it, a “pirate” site. . .”<sup>163</sup> Such a site would be obviously infringing if it contained words such as “pirate” or “bootleg” to make its illegal purpose obvious.<sup>164</sup> Of the many thousands of MP3 titles viewed by this author, none has ever been seen to contain such incriminating words. The *Commerce Committee Analysis* notes that the infringing nature of such pirate sites can be apparent from even “a brief and casual viewing,” but also implies that such a viewing is not required given that the ISP has “no obligation to seek out copyright infringement.”<sup>165</sup> The *Commerce Committee Analysis* also states that “[t]he provider could not be expected, during the course of its brief cataloguing visit, to determine whether the [item] was still protected by copyright or was in the public domain.”<sup>166</sup> Finally, in discussing a subsequent Title II provision, the *Commerce Committee Analysis* reiterates that “the Committee does not intend this provision to undermine the . . .knowledge standard. . .by suggesting that a provider must investigate possible infringements, monitor its service, or make difficult judgments as to whether conduct is or is not infringing.”<sup>167</sup>

Without an obligation on Napster’s part to seek out copyright infringement through its service, and without sufficiently blatant use of terminology by Napster users indicating their pirating activity, Napster

---

161. *A&M Records v. Napster, Inc.*, No. 99-5183 (N.D. Cal. filed Dec. 6, 1999), at para. 1.

162. H.R. REP. NO. 105-551, pt. 1 (1998), available in 1998 WL 261605, at \*65.

163. H.R. REP. NO. 105-551, pt. 2 (1998), available in 1998 WL 414916, at \*146.

164. *Id.* at \*147.

165. *Id.* at \*144.

166. *Id.* at \*146.

167. *Id.* at \*152.

should be able to prove a lack of knowledge of infringing activity if it must eventually defend itself under the Information Location Tool category.

(ii) *Removal of Infringing Material Upon Knowledge of Infringement*

Napster argues that it has done what is expected of it under Title II to prevent copyright infringement through its service. It has posted a detailed copyright policy that states that it will not tolerate infringing activities and will attempt to halt such activities if properly notified.<sup>168</sup> It has also assigned, in accordance with DMCA requirements, an individual to serve as the Designated Copyright Agent, and provides a notice form to be submitted to this Agent if copyright violations are observed.<sup>169</sup> Napster's readiness to cut service to infringers following proper notification was demonstrated on May 10, 2000, when the company blocked access to 317,377 people who had been identified by the heavy-metal rock band Metallica as offering its music illegally through Napster.<sup>170</sup>

The RIAA argues that Napster's compliance with procedural requirements to remove infringing users merely adheres to the letter of the law, not its spirit. All Napster does to remove copyright infringing users is to deny them access under their old identification names rather than blocking their entire IP address.<sup>171</sup> This enables infringing users to merely log back on under a new identification name.<sup>172</sup>

Given that Napster blocks user access upon proper notification, it should be deemed to satisfy the requirements of § 512(d)(1)(C). Banning a specific IP address, as the RIAA has suggested, would be ineffective because IP addresses are usually assigned randomly as people log onto their ISP. To block an individual by his "dynamic" IP address would require blocking everybody who uses his same ISP, potentially thousands of people. That individual could always sign up with another ISP to bypass blockage of his original ISP.

---

168. See Napster Copyright Policy (visited Apr. 27, 2000) <<http://www.napster.com/dmca.html>>. [hereinafter Napster] *But see* Opinion of Judge Marilyn Hall Patel on Def. Napster, Inc.'s Mot. For Summ. Adj. On the Applicability of the 17 U.S.C. § 512(a) Safe Harbor Affirmative Defense (N.D. Cal. 2000) (No. C99-05183 MHP), at 13 [hereinafter, Patel Opinion] (noting that Napster may not have met § 512(i) given that it developed and notified its users of a formal copyright policy only after the onset of the RIAA's litigation, and that therefore this should not moot the RIAA's claim to monetary relief for past harms.).

169. See Napster, *supra* note 168.

170. See Brad King, Napster Users Get Boot, *Wired News* (visited May 10, 2000) <<http://www.wired.com/news/business/0,1367,36248,00.html>>.

171. See *Pl.'s Opp'n to Napster's Mot. for Summ. Adj.*, *supra* note 15, at 24.

172. See *id.*; <<http://www.geocities.com>> (providing *killnappy.zip*, which facilitates the removal of Napster to permit reloading with a new user id).

More persuasive, given that Napster does block the IP addresses of users who run "bots"<sup>173</sup> on its service, is that Congress has not stated how access should be "removed" or "disabled," nor has it specified whether or not this blockage should be permanent. Napster should not have to pay the price for this legislative vagueness.

*(iii) Direct Financial Benefit from Copyright Infringement*

The RIAA complaint states that Napster derives substantial financial benefit from the copyright infringement of its users. It claims that "Napster solicits advertising and . . . charges fees for advertising on Napster."<sup>174</sup> The complaint further states that Napster is "undertaking a purposeful strategy to make its company more attractive to potential advertisers and investors by increasing the number of users, and thereby the volume of plaintiffs' sound recordings available for unlawful copying and distribution."<sup>175</sup>

Napster is not currently profitable, but if Napster does eventually become profitable through revenue sources such as on-line advertising or subscription fees, will this constitute a direct financial benefit from copyright infringement by its users? Unfortunately, the answer to this question is uncertain because Title II does not provide a substantive definition for "financial benefit." This leaves it unclear when an ISP has received a direct financial benefit from infringing activities or whether such a benefit is merely tangential.<sup>176</sup> Courts typically define "financial benefit" as revenue derived directly from infringing activity.<sup>177</sup> It is difficult conceptually to attribute on-line advertising revenue or subscription fees directly to a specific copyright-infringing product, especially if many of the products being transferred via the ISP are legitimate, non-copyright infringing items.<sup>178</sup>

*(iv) Removal of Infringing Material Upon Notification of Infringement*

There is no directly infringing material that can be removed from Napster's servers, which store only the titles and locations of music files, not the files themselves. However, as noted above, Napster has in the past removed this linking information from its servers and blocked access by copyright infringers upon proper notification to its Designated Copyright

---

173. See Patel Opinion, *supra* note 168, at 14. Bots are programs that perform actions continuously, such as searching continuously for specific MP3 files. *Id.* at 16 n.8.

174. A&M Records v. Napster, Inc., No. 99-5183 (N.D. Cal. filed Dec. 6, 1999), at para. 68.

175. *Id.*

176. See Markiewicz, *supra* note 46, at 427.

177. See *id.* at 427 n. 49; see also Fonovisa, 76 F.3d at 264.

178. See *id.* at 444.

Agent.<sup>179</sup>

#### E. LEGAL CONCLUSION: NAPSTER'S ACTIVITIES ARE PROTECTED BY TITLE II

According to the preceding analysis, Napster is protected by Title II's safe harbor provisions.<sup>180</sup> At most, then, a court would be able to order Napster to block an infringing user. Napster argues that there is no need for even this limited injunctive relief given that it has proved itself willing to block access to the Napster system if notified of infringing activity.<sup>181</sup>

The Ninth Circuit ought to adhere to the substantial judicial deference given to Congress in the area of copyright law, under which courts generally refuse to unilaterally broaden copyright protections in response to technological change.<sup>182</sup> One commentator has noted that "Congress is the only body capable of answering the specific technical questions and reconciling the often competing policy interests associated with the question of liability for online copyright infringement."<sup>183</sup> Thus even if a court feels that the legislature in drafting Title II would have forbidden a system such as Napster's had it been envisioned, the court should recognize that this is not its decision to make.

### VII. IMPLICATIONS FOR THE FUTURE

#### A. TECHNOLOGICAL CAT AND MOUSE GAME

The RIAA has been "tracking and threatening pirates who, in turn, develop ever more sophisticated skill for evading this detection."<sup>184</sup> Thus even if the RIAA emerges victorious from its dispute with Napster, its triumph will be short-lived. Napster's method for facilitating MP3 transfers has already been reproduced by systems such as iMesh,<sup>185</sup> CuteMX,<sup>186</sup> and SpinFrenzy.<sup>187</sup> Any system such as these could quickly fill the void left by Napster's disappearance, and from abroad, if necessary, to get beyond the reach of American copyright law.

Even without Napster's system in place, copyright infringement in the digital age is so widespread that enforcement is nearly impossible.

179. See King, *supra* note 170.

180. See *id.*

181. *Napster's Mot. for Summ. Adj.*, *supra* note 81, at 22.

182. See Davis, *supra* note 37.

183. Skelton, *supra* note 68, at 314.

184. Barak D. Jolish, *Scuttling the Music Pirate: Protecting Recordings in the Age of the Internet*, 17 ENT. & SPORTS L. 9, 10 (1999).

185. See <<http://www.imesh.com>> (visited Apr. 27, 2000).

186. See <<http://www.cuteftp.com/products/cutemx>> (visited Apr. 27, 2000).

187. See <<http://www.spinfrenzy.com/stuff/welcome.asp>> (visited Apr. 27, 2000).

Traditional pirate web sites that store infringing material are already difficult to find because they appear and disappear so quickly. Aficionados of pirated music frequently use Internet Relay Chat forums to advise one another of short-term postings of illegal music archives.<sup>188</sup> Attempting to track down and sue such fleeting entities is not financially feasible for the music industry. As Ryan Henriquez has noted, “while the industry navigates its victory over one online music provider, numerous other pirates have already begun their infringing activities, and it is simply impossible for the music industry to locate and stamp out every instance of infringement.”<sup>189</sup>

The music industry’s much-heralded Secure Digital Music Initiative (SDMI) will also be unable to stop piracy. In December 1998, a consortium comprised of the RIAA, Universal, Sony, Bertelsmann, EMI, Time-Warner, the International Federation of Phonographic Institutes, and various technology companies launched SDMI to develop technology that would prevent unauthorized copies of digital music.<sup>190</sup> As envisioned, SDMI would either encrypt music or attach a copyright management system into a music file and travel with the file over the Internet.<sup>191</sup> What the SDMI consortium overlooks is that for every obstacle one can erect, a counter-technology will be developed if the information content is valuable enough. This can occur either through hardware or software modifications.

From a hardware perspective, controlling information flow is difficult when dealing with personal computers, which are designed with an open architecture. Given that nearly every computer component can be replaced by the user, decrypted information “can be captured in numerous ways as it passes from one place to another inside the machine.”<sup>192</sup> For example, one could easily modify the functioning of the sound card so that it not only generates the signal for the speakers but also stores the music file onto the hard drive.<sup>193</sup>

With regard to software, the battle against piracy will be equally difficult. Software systems superior to Napster have already been devel-

---

188. See Parker Interview, *supra* note 16.

189. Ryan S. Henriquez, *Facing the Music on the Internet: Identifying Divergent Strategies for Different Segments of the Music Industry in Approaching Digital Distribution*, 7 UCLA ENT. L.R. 57, Fall 1999, at 78.

190. See *id.* at 87; Jonathan Vankin, *Downloading the Future: The MP3 Revolution—the End of the Industry as We Know It*, L.A. WEEKLY, Mar. 26, 1999, at 36.

191. See Henriquez, *supra* note 189, at 83.

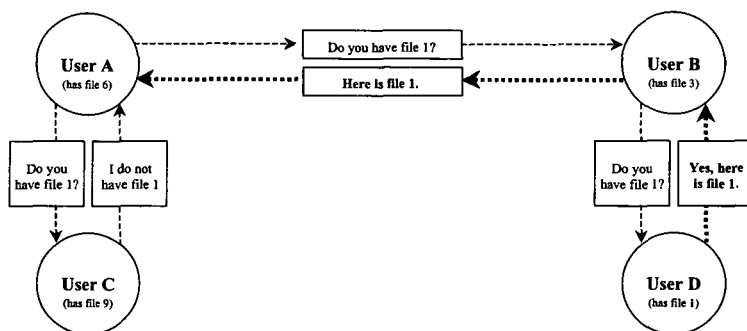
192. See National Research Council, *The Digital Dilemma - Intellectual Property in the Digital Age—Ch. 2* (visited Apr. 27, 2000) <[http://books.nap.edu/html/digital\\_dilemma/ch2.html](http://books.nap.edu/html/digital_dilemma/ch2.html)> [hereinafter NRC - Ch.2].

193. See *id.*

oped, though they are not yet widely used.<sup>194</sup> Unlike Napster, which is “semi-tiered”<sup>195</sup> and therefore has a central server, the future of information flows could lie with anonymous, “non-tiered”<sup>196</sup> systems that avoid the need for a central server.<sup>197</sup> Systems such as SafeX,<sup>198</sup> Gnutella,<sup>199</sup> FreeNet,<sup>200</sup> and Publius<sup>201</sup> provide greater user privacy, are relatively impervious to hacker attack, and in some cases employ intelligent routing and caching to improve transmission efficiency.<sup>202</sup>

A description of how non-tiered systems operate is best done by example. Suppose User A is seeking a specific file (File #1). User A only trusts Users B and C to know that he is seeking this information, either because User A lives in a country that vigorously prosecutes copyright infringers, or because User A lives in a totalitarian state that will disapprove of his obtaining certain information via computer. User A asks Users B and C if they have File #1. Unfortunately, they do not, but User B knows User D and asks him if he has File #1. User D does have File #1 and immediately transfers it to User B, who immediately forwards it to User A. Because the system is anonymous, User A will never know that the file came originally from User D. This process is depicted in the following chart.

### Non-Tiered File Transfers



194. See Thomas E. Weber, *Maverick Programmers Prepare to Unleash Anarchy on the Web*, WALL ST. J., Mar. 27, 2000, at B1.

195. See Telephone Interview with Jonathan Berschadsky, Patent Attorney (Mar. 22, 2000). Semi-tiered systems involve direct user-to-user interaction following a small amount of initial assistance by a central server.

196. See Weber, *supra* note 194; See also Free Network Project, *supra* note 195. Such systems are also known as fully distributed, peer-to-peer, or decentralized.

197. See Weekly Interview, *supra* note 18.

198. Acronym for Secure Anonymous File Exchange. See *id.*

199. See <<http://gnutella.wego.com>> (visited Apr. 27, 2000).

200. See Free Network Project (visited Apr. 27, 2000) <<http://freenet.sourceforge.net>>.

201. See *id.* Publius is currently under development.

202. See Free Network Project, *supra* note 200.

As can be seen, file transfers via a non-tiered system are made anonymously and only from trusted parties. Even if an Internet copyright pirate could be identified, he would most likely just be an individual without deep pockets—an undesirable defendant to a plaintiff seeking a large monetary award for copyright infringement. With this kind of technology poised for widespread implementation, Napster officials are surprised that the RIAA has no interest in entering into some sort of commercial arrangement with a semi-tiered system such as Napster, where a central server can at least be identified (and negotiated with).<sup>203</sup> By suing Napster, the RIAA will only succeed in opening the doorway further to non-tiered systems.

### B. PARADIGM SHIFT IN THE MUSIC INDUSTRY

New technology is frequently perceived as a destroyer of the existing market. In 17th century England, for example,

. . . the emergence of lending libraries was seen as the death knell of book stores; in the 20<sup>th</sup> century, photocopying was seen as the end of the publishing business, and videotape the end of the movie business. Yet in each case, the new development produced a new market far larger than the impact it had on the existing market. Lending libraries gave inexpensive access to books that were too expensive to purchase, thereby helping to make literacy widespread and vastly increasing the sale of books.<sup>204</sup>

Similarly, photocopies have not destroyed the market for books, and videotaping has actually increased movie-watching.<sup>205</sup> But in each case the original market was transformed, “in some cases bringing a new cast of players and a new power structure.”<sup>206</sup> This process of transformation can be traumatic to those who depend financially upon the *status quo*.

The RIAA has resisted technological progress in the audio field over the past decade, justifying its actions by arguing that “recording artists would be deprived of copyright fees.”<sup>207</sup> It squelched the Digital Audio Tape (DAT) market by lobbying for the AHRA, which imposed a 2% royalty on the sale of each DAT recorder and required imposition of SCMS anti-copying technology.<sup>208</sup> It tried unsuccessfully to prevent Diamond Multimedia’s introduction of the Rio MP3 recorder. Currently the RIAA is focusing on Internet-based copyright infringement and has success-

---

203. See Parker Interview, *supra* note 16.

204. See NRC - ch.2, *supra* note 192 (quoting from Carl Shapiro and Hal R. Varian, INFORMATION RULES: A STRATEGIC GUIDE TO THE NETWORK ECONOMY (1998)).

205. *Id.*

206. See *id.*

207. Kover, *supra* note 27, at 129.

208. See *id.*



fully shut down hundreds of websites trafficking in pirated music.<sup>209</sup> The music industry thus appears unwilling to adapt to changing times, suggesting that it has become too comfortable doing things the same old way. As Jim Griffin, former Technology Director for Geffen Records, has stated, "No wonder the business is scared. It's going to have to reinvent itself from the ground up, and that process is going to be a painful one."<sup>210</sup>

Given the music industry's rigidity, it is likely that the artists themselves will take the lead in transforming the way music is distributed. Many have already come to realize that the music industry offers little in return for the 88 cents on the dollar it extracts from the sale of every CD.<sup>211</sup> Chuck D. of the rap group *Public Enemy* notes that ". . .the record companies have been getting away with murder for 12 years, since the advent of the CD, when they could manufacture something for 69 cents and sell it for \$10.98 wholesale."<sup>212</sup> There are several new business models that the record industry, individual performance artists, and on-line music distributors should consider:

#### 1. *Low-Priced Distribution with Convenient Purchasing*

This model holds that music should be sold cheaply over the Internet because "the low price and ease of purchase make it more attractive to buy than to copy."<sup>213</sup> Michael Robertson, President and CEO of MP3.com, believes that "[s]ome music fans will always copy songs illegally. . .but if you make it easy enough for them to pay for music on the Net, the majority of them will."<sup>214</sup> Barak Jolish recommends:

. . . a new business model which would focus on delivery of digital music over the Web at prices substantially lower than today's retail rates. When combined with low price, the convenience of established industry web sites might offset the consumer's incentive to engage in piracy in the first place. Consumers who know that, for instance, they legally can obtain the single they want for 50 cents may not bother searching through unreliable pirate sites for the same music. In other words, consumers may be willing to forgo the marginal savings of pirate sites in exchange for the industry site's superior convenience and service.<sup>215</sup>

---

209. See Janelle Brown, *Heat Turned Up on Digital Music Pirates*, Wired.com (Feb. 12, 1998) <[http://www.wired.com/news/print\\_version/email/member/culture/story/10234.html](http://www.wired.com/news/print_version/email/member/culture/story/10234.html)>.

210. Dibbell, *supra* note 10, at 106.

211. See Vankin, *supra* note 190, at 36.

212. *Id.* at 38.

213. National Research Council, *The Digital Dilemma - Intellectual Property in the Digital Age—Exec. Summ.* (visited Apr. 27, 2000) <[http://books.nap.edu/html/digital\\_dilemma/exec\\_summ.html](http://books.nap.edu/html/digital_dilemma/exec_summ.html)>.

214. See Dibbell, *supra* note 10, at 106.

215. See Jolish, *supra* note 184, at 12.

In this regard, the music industry can learn an important lesson from the experience of the software industry, which for years “experimented with a variety of copy-protection mechanisms, trying desperately to come up with a scheme that consumers would put up with, but in the end. . .admitted defeat. Copy protection just adds friction to a product whose chief value is its frictionlessness.”<sup>216</sup> The software industry eventually learned to live with a certain amount of piracy, and is currently quite profitable.<sup>217</sup> Jolish argues that the music industry can also continue to be profitable in the digital age, especially given the costs it can save.

First, distributing music on the Internet would eliminate the expense of pressing CDs, shipping them to the United States, delivering them to a store, and many other costs associated with retail sales outlets. Second, the convenience of online delivery and the new attractive pricing may increase sales volume. The number of impulse buys, for instance, undoubtedly would rise.<sup>218</sup>

One website that has adopted this model is GoodNoise, which sells songs online for 99 cents each.<sup>219</sup> These songs are usually by known, though not upper-tier, artists.<sup>220</sup> GoodNoise splits its profits 50-50 with the artists whose music is distributed on its site.<sup>221</sup> Steve Grady, GoodNoise Vice-President for Marketing, states that “[t]he 99 cents is to some extent a convenience fee. We want to make it easier for the consumer to buy the music than to steal it. If you do that effectively, there’s a great business there.”<sup>222</sup>

## 2. *Mass Customization*

The idea of selling songs individually could be seen as a precursor to the mass customization model already applied by many other industries. These industries try to give customers more choices by breaking down their product into its fundamental components, thereby allowing consumers to customize their own solutions.<sup>223</sup> For example, the article you are reading was typed on a computer manufactured by Dell, which permitted the author to select the size of the hard drive, the amount of random-access memory (RAM), the microprocessor speed, the pre-installed

---

216. See Dibbell, *supra* note 10, at 106.

217. See *id.* at 106.

218. *Id.*

219. See Vankin, *supra* note 190, at 36; see also EMUSIC, (visited Apr. 27, 2000) <<http://www.goodnoise.com>>.

220. See Vankin, *supra* note 190, at 36.

221. See *id.*

222. See *id.*

223. See Allen Weiss, *Learning From Napster*, UPSIDE TODAY, Mar. 28, 2000, available in 2000 WL 4724569.

software bundle, the type and speed of the modem, etc. Dell understands that customers increasingly demand the ability to configure the product they buy.

The music industry, on the other hand, has never embraced the concept of mass customization, which would enable consumers to select specific songs by different artists and then record them onto a customized CD.<sup>224</sup> Instead, the music industry continues to expect people to pay up to \$18 for a CD that in some cases contains no more than one or two desired songs.

Widespread piracy often indicates an unmet customer need. The need here is for flexibility. Though MP3s enable customers to bypass the music industry's rigidity by engaging in their own product customization, it may not be too late for the industry to adapt and regain some lost ground. By enabling consumers to easily customize the CDs they purchase, the music industry might succeed in taking some of the wind out of the pirates' sails.

### 3. *Advertiser-Support*

This model, which can work in tandem with the Low-Price Mass Distribution model described above, operates by pricing music low or even giving it away for free. Revenue is generated through paid advertisements directed towards purchasers browsing the Internet to obtain music.<sup>225</sup> Many websites currently operate profitably under such a model.

### 4. *Record Companies as Information Providers*

Under this model, what is today considered "music piracy" would become openly and legally practiced. MP3 files would be freely available throughout the Internet, with performers generating revenues through live performances rather than recordings. Composers would receive royalties from revenues generated by the performers. Traditional CD manufacturers and distributors will have been disintermediated because performers would now be independently distributing their products online without the assistance of record companies.

Free access to information, however, will likely lead to information overload.<sup>226</sup> Consumers will be unable to determine which music is worth listening to, and for artists, getting noticed will become more crucial than ever.<sup>227</sup> The music industry, having left its traditional role of physical intermediary, would now assume the role of informational inter-

---

224. *See id.*

225. *See* Vankin, *supra* note 190, at 40.

226. *See id.*

227. *See id.*

mediary by directing consumers to “better” music. It would generate revenue through advertising or subscription fees to its proprietary websites.

#### VIII. CONCLUSION

The RIAA’s lawsuit against Napster has the potential to define the parameters of what constitutes copyright infringement in the Internet age. But regardless of the outcome of this particular case, the rapid pace of technological change will continue and make it increasingly difficult for the legal system to protect the *status quo* of the music industry. If the industry wishes to survive in this new era, it will be forced to adopt a more viable business model—one that enables it to embrace the Internet rather than resist the opportunities it offers.

