Loyola of Los Angeles
Entertainment Law Review

Volume 22 | Number 1 Article 2

6-1-2001

Post-Napster: Peer-to-Peer File Sharing Systems Current and Future Issues on Secondary Liability under Copyright Laws in the United States and Japan

Hisanari Harry Tanaka

POST-NAPSTER: PEER-TO-PEER FILE SHARING SYSTEMS CURRENT AND FUTURE ISSUES ON SECONDARY LIABILITY UNDER COPYRIGHT LAWS IN THE UNITED STATES AND JAPAN

Hisanari Harry Tanaka[*]

I. INTRODUCTION

A. The Issues

On February 12, 2001, the United States Court of Appeals for the Ninth Circuit issued an opinion on appeal from the United States District Court for the Northern District of California, granting plaintiffs' motion for a preliminary injunction against Napster, Inc. ("*Napster IV*").[1]

The entertainment industry, represented in this case by several record companies, has repeatedly sued for copyright infringement resulting from the rapid development of digital technology and the Internet.[2] Digital technology enables the transformation of copyrighted works into digital contents.[3] The Internet has allowed people to become independent distributors

---

* Lawyer-from-Abroad, Covington & Burling, September 2001–. LL.M. on Trade Regulation (Intellectual Property Law), New York University, May 2001. Qualified to practice in Japan as *bengoshi*, specializing in intellectual property, technology, and litigation. Please send comments to hisanari_tanaka@hotmail.com. The author would like to thank Professor Neil Netanel of the University of Texas School of Law who instructed the author in preparing this Article as part of the Advanced Copyright Problems seminar held at NYU in the spring of 2001. Many thanks also to Sarah Iles for her thorough comments and kind encouragements.

1. A & M Records, Inc. v. Napster, Inc., 239 F.3d 1004, 1029 (9th Cir. 2001).

2. Consider the past year where members of the music industry, represented by the Recording Industry Association of America ("RIAA"), have sued, among others, Scour and MP3.com for copyright infringement. Press Release, Scour, Motion Picture and Music Industries File Suit Against Scour.com (July 20, 2000), *at* http://www.mpaa.org/press/scourpressrelease.htm; UMG Recording, Inc. v. MP3.com, Inc., 92 F. Supp. 2d 349 (S.D.N.Y. 2000).

3. The Cross-Industry Working Team, *Managing Access to Digital Information: An Ap-*

of copyrighted works because they can distribute digital contents all over the world instantaneously with just a minimal investment—a personal computer and Internet connection.[4] The market for digital content distribution is expected to reach 5.95 billion dollars by the year 2005.[5]

The *Napster* cases may come to be seen as a milestone—the first of a new type of digital battle fought by content providers represented by the entertainment industry.[6] Although Napster is showing its willingness to comply with the preliminary injunction issued on March 5, 2001,[7] there are concerns that new capabilities derived from or modeled after Napster could continue to provide similar services to Napster's refugee customers.[8] These services are based on a "peer-to-peer network" or "file sharing system" architecture ("P2P").[9] P2P technologies are gaining popularity, with the potential for new business architecture on the bright side, and unauthorized reproduction and dissemination of copyrighted works on the dark side.[10]

The *Napster* cases represent the dark side of P2P technologies. Because P2P technologies enable direct file sharing between individual users without relying on a central server that stores or routes digital contents, the direct infringement occurs at the level of the individual.[11] Therefore, it is unclear as to whether P2P service providers could be held liable under a theory of secondary liability. If service providers cannot be held liable for a theory of secondary liability, content providers will be forced to face the more difficult task of holding individual users liable to enforce their copyrights.[12]

There is also concern over the cross-border, international aspect of P2P networking. Digital technology and the Internet inevitably possess potential copyright infringement capabilities that involve cross-border trans-

---

proach Based on Digital Objects and Stated Operations, 6 J. PROPRIETARY RTS. 2 (1997), WL 9 No. 6LPROPR2.

4. *Id.*

5. Press Release, Aberdeen Group, Digital Content Distribution Market to Reach $5.95 Billion by 2005 (Mar. 30, 2001), *at* http://www.aberdeen.com/ab%5fcompany/press/03%2030%2d01dcd.htm.

6. *See generally* Harrison J. Dossick & David Halberstadter, *Facing the Music*, L.A. LAW., Apr. 2001, at 34, 36 [hereinafter *Facing the Music*] (discussing the future implications of the *Napster* cases).

7. A & M Records, Inc. v. Napster, Inc., No. C 99-05183 MHP, 2001 U.S. Dist. LEXIS 2186 (N.D. Cal. Mar. 5, 2001).

8. *Facing the Music*, *supra* note 6, at 39.

9. A & M Records, Inc. v. Napster, Inc., 114 F. Supp. 2d 896, 902 (N.D. Cal. 2000).

10. *See id.* at 902–03.

11. *See id.* at 907.

12. *See* A & M Records, Inc. v. Napster, Inc., 239 F.3d 1004, 1027 (9th Cir. 2001).

actions or interactions.[13] Thus, Napster or similar post-Napster P2P services can easily set up servers or build networks in other countries.[14]

Part I of this Article discusses the background and technology necessary to correctly understand the issues. Part II reviews the central *Napster* opinions and analyzes rules that can be drawn from the decision with respect to secondary liabilities, i.e., contributory infringement and vicarious infringement of service providers. Part III applies these rules to post-Napster P2P services, systems, and networks, including centralized P2P and decentralized P2P. Part IV contends that Napster-like P2P services are likely to be liable under Japanese laws. Part V argues that technological enforcement will be indispensable in the support of legal enforcement. Finally, Part VI concludes that thriving P2P and technological advancement in connection with computers and the Internet will force content providers to rely on technology to enhance their ability to protect their copyrights. In order to address the problems spawned by digital technology, those problems must be resolved by digital technology.

B. Procedural History of Napster

A lawsuit was filed on December 6, 1999 charging Napster with contributory and vicarious copyright infringement ("*Napster III*").[15] The plaintiffs are record companies engaged in the commercial recording, distribution, and sale of copyrighted musical compositions and sound recordings.[16] On July 26, 2000, the district court granted plaintiffs' motion for a preliminary injunction.[17] The injunction was slightly modified by a written opinion on August 10, 2000.[18] The district court enjoined Napster "from engaging in, or facilitating others in copying, downloading, uploading, transmitting, or distributing plaintiffs' copyrighted musical compositions and sound recordings, protected by either federal or state law, without express permission of the rights owner."[19] Napster appealed ("*Napster II*").[20]

---

13. *Facing the Music*, *supra* note 6, at 39.

14. *Id.* P2P services, such as iMesh in Israel, locate central servers outside the United States and attract numerous users from around the world, including the United States. *See* John Borland, *Napster Alternatives Start Blocking Songs*, CNET NEWS.COM (Apr. 6, 2001), *at* http://news.cnet.com/news/0-1005-200-5530715.html [hereinafter *Napster Alternatives Start Blocking Songs*].

15. A & M Records, Inc. v. Napster, Inc., 114 F. Supp. 2d 896, 900 (N.D. Cal. 2000).

16. *Id.*

17. *Id.* at 927.

18. *See id.*

19. *Id.*

20. A & M Records, Inc. v. Napster, Inc., No. 00-16403, 2000 U.S. LEXIS 18688 (9th Cir. July 28, 2000).

The appellate court then entered a temporary stay of the preliminary injunction pending resolution of the appeal.[21]

On February 12, 2001, the U.S. Court of Appeals for the Ninth Circuit affirmed in part, reversed in part, and remanded the case.[22] Nonetheless, the court upheld the preliminary injunction against Napster.[23]

On March 5, 2001, the district court issued a preliminary injunction order ("Order") in accordance with the opinion of the Ninth Circuit.[24] The Order required Napster to block the traffic of all copyrighted sound recordings whose title and artist name were provided by the plaintiffs.[25] In other words, Napster was required to prevent transmission of any files that purportedly contained these sound recordings.

C. The P2P Technology: How Napster Works

1. P2P Technology

Digitizing[26] copyrighted works ("contents" or "digital contents") allows those works to be distributed over the Internet.[27] Digital contents, such as music and songs on compact discs ("CDs") or movies on digital versatile discs ("DVDs"), have been widely distributed over the Internet mainly by individuals.[28] Digital contents are typically distributed or acquired over the Internet via downloading or streaming methods.[29] Generally, in order to share files, Internet users must upload contents to a server[30] that stores the contents and enables others to browse or download[31] the con-

---

21. *Id.* at *2.

22. A & M Records, Inc. v. Napster, Inc., 239 F.3d 1004, 1029 (9th Cir. 2001).

23. *Id.*

24. A & M Records, Inc. v. Napster, Inc., No. C 99-05183 MHP, 2001 U.S. Dist. LEXIS 2186, *7–*8 (N.D. Cal. Mar. 5, 2001).

25. *Id.*

26. "Digitizing" refers to the translation of data into digital form so that computers can process it. *See What is Digitizing?*, *at* http://www.sunfishstudios.com/digitizing.htm (last visited Sept. 17, 2001).

27. A & M Records, Inc. v. Napster, Inc., 114 F. Supp. 2d 896, 901 (N.D. Cal. 2000).

28. For the purpose of this Article, unless otherwise noted, contents or digital contents shall indicate digitized music and songs.

29. A & M Records, Inc. v. Napster, Inc., 114 F. Supp. 2d 896, 901 (N.D. Cal. 2000).

30. *See id.* "In general, a server is a computer program that provides services to other computer programs in the same or other computers." *Server—A SearchEnterpriseServers Definition*, *at* http://searchenterpriseservers.techtarget.com/sdefinition/0,,sid25_gci2129964,00.html (last visited Oct. 13, 2001). A computer that runs a server program is also frequently referred to as a "server" though it may contain a number of server and client programs. *Id.*

31. *See* ROBIN WILLIAMS & STEVE CUMMINGS, JARGON, AN INFORMAL DICTIONARY OF COMPUTER TERMS 170–71 (Peachpit Press, Inc. 1993). "To download means to receive informa-

tents by means of FTP or HTTP.[32] Napster, Gnutella, and other P2P systems, however, enable one Internet user to directly access another individual user's hard drive and download any files that are offered for sharing without relying on a particular central server for storage.[33] P2P architecture creates a network in which each individual computer has equivalent capabilities and responsibilities by maintaining both distribution functions and receiving functions (server *plus* client).[34] This differs from client-server architectures in which some computers primarily function as servers.[35] In a P2P network, information and contents are transmitted between users in the network.[36] Therefore, P2P networks use up significant bandwidth on the Internet.[37] However, the rapid developments of broadband and high-speed Internet connections have enabled the P2P system to become viable for large numbers of individual users.[38]

2. How Napster Works

Napster has designed and operates a system that permits the transmission and retention of sound recordings employing digital technology.[39] An MP3[40] file is created through a process colloquially known as ripping and

---

tion, typically a file, from another computer to yours via your modem . . . . The opposite term is upload, which means to send a file to another computer." *Id.*

32. *Hypertext Transfer Protocol—A SearchSystemsManagement Definition, at* http://searchsystemsmanagement.techtarget.com/sdefinition/0,,sid20_gci2149994,00.html (last updated Oct. 5, 2000); *see also File Transfer Protocol—A SearchSystemsManagement Definition, at* http://searchnetworking.techtarget.com/sdefinition/0,,sid_gci213976,00.html (last updated Feb. 7, 2001).

33. A & M Records, Inc. v. Napster, Inc., 239 F.3d 1004, 1011–12 (9th Cir. 2001). Napster has a central server that indexes file location and information. *See id.* However, such a server does not store the contents for users. *See id.*

34. *See* John Borland & Mike Yamamoto, *The P2P Myth*, CNET NEWS.COM (Oct. 26, 2000), *at* http://news.cnet.com/0-1005-201-3248711-2.html [hereinafter *The P2P Myth*].

35. *See id.*

36. *See id.*

37. *See id.* P2P networks, especially decentralized P2Ps like Gnutella, are vulnerable to traffic jams created by one personal computer with a dial-up connection because the data is routed from computer to computer. *Id.*

38. While Napster's service only facilitates exchange of MP3 files, users of many other P2P services can exchange files in other formats, including file formats supporting video. *Id. See generally infra* note 40 (defining "MP3").

39. A & M Records, Inc. v. Napster, Inc., 239 F.3d 1004, 1011 (9th Cir. 2001).

40. "MP3" refers to the file format standard set in 1987 by the Moving Picture Experts Group of the International Organization for Standardization ("ISO"). *Id.* Layer 3 is one of three coding schemes for the compression of video and audio signals. *MP3—Webopedia Definition and Links, at* http://webopedia.internet.com/term/m/MP3.html (last visited Sept. 6, 2001). The compression makes the original wave file ripped from a compact disc ("CD") approximately twelve times smaller without sacrificing its sound quality. *Id. See generally infra* note 43 (defin-

encoding.[41] Ripping and encoding software[42] allows a computer owner to copy sound sequence data as wave[43] files from CDs directly onto a computer's hard drive and subsequently compress the audio information into the MP3 format.[44] The MP3 compression format allows rapid transmission of audio files between computers by electronic mail or any other FTP.[45] Napster facilitates the transmission of MP3 files between its users:

> Through a process commonly called "peer-to-peer" file sharing, Napster allows its users to: (1) make MP3 music files stored on individual computer hard drives available for copying by other Napster users; (2) search for MP3 music files stored on other users' computers; and (3) transfer exact copies of the contents of other users' MP3 files from one computer to another via the Internet.[46]

However, the P2P file sharing process has to be distinguished from uploading the files to the Napster server on the Internet. Although the file information, *i.e.*, file name and file type, would be sent to the immediate server, the copyrighted works are never copied or transferred to the Napster server.[47] These functions are made possible by Napster's MusicShare software, which is available free of charge from Napster's website, and Napster's network servers and server-side software.[48] In addition to other functions, "Napster provides technical support for the indexing and searching of MP3 files . . . including a chat room, where users can meet to discuss music, and a directory where participating artists can provide information about their music."[49]

II. THE *NAPSTER* OPINION

In *Napster IV*, the panel addressed the following issues: (1) direct copyright infringement by users; (2) the fair use defense against the charge of direct infringement by users; (3) demonstrated defenses to contributory

---

ing "wave" file).

41. *Id.*

42. *See MP3.com Software*, http://software.mp3.com/software/featured/windows/rippers/?cp=hw_main.html (last visited Sept. 6, 2001).

43. A "wave" file is "an audio file format, created by Microsoft." *Wav—A Whatis Definition*, *at* http://whatis.techtarget.com/definition/0,,sid9_gci213473,00.html (last visited Sept. 13, 2001). It has become a standard audio file format for computer system and game sounds. *Id.*

44. A & M Records, Inc. v. Napster, Inc., 239 F.3d 1004, 1011 (9th Cir. 2001).

45. *Id.*

46. *Id.*

47. *See id.* at 1012.

48. *Id.* at 1011.

49. *Id.*

infringement claims, such as sampling, space-shifting, and permissive distribution of recordings by artists; (4) vicarious infringement claims; (5) applicability of the Audio Home Recording Act ("AHRA");[50] (6) applicability of the safe harbor provision under the Digital Millennium Copyright Act ("DMCA")[51] to limit liability for contributory and vicarious infringement; and (7) waiver, implied license and copyright misuse as other defenses.[52] This Article will focus only on those issues that deal with Napster's secondary liability and the applicability of the DMCA safe harbor provision to Napster as a P2P service provider.[53]

A. Secondary Liability of Napster

Secondary liability for copyright infringement does not exist in the absence of direct infringement by a third party.[54] It follows that Napster cannot facilitate infringement of copyright law in the absence of direct infringement by its users.[55] The panel concluded that the plaintiffs held copyrights in a substantial number of works exchanged by the Napster system.[56] The panel held that Napster users, when they upload file names to the search index for others to copy, violate the plaintiff's distribution rights[57] and violate the plaintiff's reproduction rights when they download files containing copyrighted music.[58] Napster asserted that its users do not directly infringe plaintiffs' copyrights because "the users are engaged in

50. Pub. L. No. 102-563, 106 Stat. 4237 (1992) (codified in scattered sections of 17 U.S.C.).

51. Pub. L. No. 105-304, 112 Stat. 2860 (1998) (codified in scattered sections of 17 U.S.C.).

52. A & M Records, Inc. v. Napster, Inc., 239 F.3d 1004, 1011 (9th Cir. 2001).

53. The panel rejected the argument that under the AHRA, MP3 file exchange is a type of "noncommercial use" for making digital musical recordings protected from infringement actions by the statute on the grounds that: (1) computers and hard drives are not "digital audio recording devices" because their "primary purpose" is not to make digital audio copied recordings and (2) "digital musical recording" does not include songs fixed on computer hard drives. *Id.* at 1024 (citing Recording Indus. Ass'n of Am. v. Diamond Multimedia Sys., Inc., 180 F.3d 1072, 1077–78 (9th Cir. 1999)). The Panel dismissed the remaining affirmative defenses of waiver, implied license, and copyright misuse. *Id.* at 1026–27.

54. Religious Tech. Ctr. v. Netcom On-Line Communication Servs., Inc., 907 F. Supp. 1361, 1371 (N.D. Cal. 1995) (stating "there can be no contributory infringement by a defendant without direct infringement by another").

55. A & M Records, Inc. v. Napster, Inc., 239 F.3d 1004, 1013 (9th Cir. 2001). Napster did not appeal the district court's conclusion that the plaintiffs presented a prima facie case of direct infringement by Napster users. *Id.* at 1013.

56. *See id.*

57. *Id.* at 1014. The panel's decision arguably begs the question of whether the plaintiffs' distribution rights include the uploading of an index containing only file names referring to their works. *See id.*

58. *Id.*; *see* 17 U.S.C. § 106 (1994); *see also id.* § 501(a) (1994) (Infringement occurs when alleged infringer engages in activity listed in § 106.).

fair use of the material."[59] However, the panel rejected Napster's fair use defense.[60]

B. Contributory Liability

Unlike patent law,[61] the U.S. Copyright Act[62] ("Copyright Act") does not have a provision for contributory infringement. The Supreme Court, however, recognizes the absence of such a provision does not preclude the finding of contributory infringement under copyright law.[63] The panel concluded that Napster knowingly encourages and assists its users in infringing the record companies' copyrights and materially contributes to the infringing activity.[64] Because liability for contributory infringement requires knowledge of and material contribution to the infringement,[65] the panel's findings meant that the plaintiffs established the two elements of a prima facie case for contributory infringement.[66] The panel concluded that if a computer system operator learns that specific infringing material is available on the system, and fails to purge such material from the system, the operator knows of and contributes to direct infringement.[67] Knowledge

59. A & M Records, Inc. v. Napster, Inc., 239 F.3d 1004, 1014 (9th Cir. 2001). (stating "Napster identifies three specific alleged fair uses: sampling, where users make temporary copies of a work before purchasing; space-shifting, where users access a sound recording through the Napster system that they already own in audio CD format; and permissive distribution of recordings by both new and established artists").

60. *See id.* at 1015. Four factors that are to be used for fair use determination are "(1) the purpose and character of the use . . . (2) the nature of the copyrighted work; (3) the amount and substantiality of the portion used in relation to the copyrighter work as a whole; and (4) the effect of the use upon the potential market for the work or the value of the work." *Id.*; *see also* 17 U.S.C. § 107 (1994). The panel supported the district court's conclusion that downloading MP3 files does not transform the copyrighted work. A & M Records, Inc. v. Napster, Inc., 114 F. Supp. 2d 896, 912 (N.D. Cal. 2000). Courts have been reluctant to find fair use when an original work is merely retransmitted in a different medium. A & M Records, Inc. v. Napster, Inc., 239 F.3d 1004, 1015 (9th Cir. 2001). Additionally, the panel agreed with the district court's findings that Napster users were engaged in commercial use, which is demonstrated by showing repeated and exploitative unauthorized copies of copyrighted works were made to save the expense of purchasing authorized copies. *Id.*

61. *See generally* 35 U.S.C. § 271(b) (1994).

62. 17 U.S.C. §§ 101–1332 (1994 & Supp. V 1999).

63. Sony Corp. of Am. v. Universal City Studios, Inc., 464 U.S. 417, 435 (1984).

64. A & M Records, Inc. v. Napster, Inc., 239 F.3d 1004, 1021–22 (9th Cir. 2001).

65. *See* Fonovisa, Inc. v. Cherry Auction, Inc., 76 F.3d 259, 264 (9th Cir. 1996) (quoting Gershwin Publ'g Corp. v. Columbia Artists Mgmt., Inc., 443 F.2d 1159, 1162 (2nd Cir. 1971)). Contributory liability requires that the secondary infringer "know or have reason to know" of direct infringement. *See* Cable/Home Communication Corp. v. Network Prods., Inc., 902 F.2d 829, 845–46 n.29 (11th Cir. 1990); *Netcom*, 907 F. Supp. at 1373–74 (framing the issue as "whether Netcom knew or should have known of" the infringing activities).

66. A & M Records, Inc. v. Napster, Inc., 239 F.3d 1004, 1020–22 (9th Cir. 2001).

67. *See Netcom*, 907 F. Supp. at 1375.

may be found if the copyright owner has informed the operator that infringing files are available in the system.[68]

Napster contended that by demonstrating "commercially significant noninfringing" uses it could not be liable for contributory infringement[69] under *Sony Corp. of America v. Universal City Studios, Inc.*[70] The panel ruled, however, that regardless of the numbers of infringing versus noninfringing uses, Napster's actual, specific knowledge of direct infringement renders the *Sony* holding of "limited assistance."[71] Conversely, absent any specific information identifying infringing activity, a computer system operator cannot be liable for contributory infringement merely because the structure of the system permits the exchange of copyrighted material.[72] In addition, *Napster IV* seems implicitly to have distinguished the Napster system from the system in *Sony* by another element—the technology purveyor's inability to control infringement.[73] The court held that the capacity to remove indices from its server and eliminate the infringing activities of the users distinguished the case from *Sony*, where manufacturers could not control users' actual use.[74] As for the material contribution element, the court agreed with the district court's conclusion that Napster provides "the site and facilities" for direct infringement by providing support services that enable the users to find and download music with ease, and that Nap-

68. A & M Records, Inc. v. Napster, Inc., 239 F.3d 1004, 1020 (9th Cir. 2001).

69. *Id.* at 1021.

70. 464 U.S. at 442–44.

71. A & M Records, Inc. v. Napster, Inc., 239 F.3d 1004, 1020–21 (9th Cir. 2001). "Regardless of the number of Napster's infringing versus noninfringing uses, the evidentiary record here supported the district court's finding that plaintiffs would likely prevail in establishing that Napster knew or had reason to know of its users' infringement of plaintiffs' copyrights." *Id.*

72. *See id.* (stating that to "enjoin simply because a computer network allows for infringing use would, in our opinion, violate *Sony* and potentially restrict activity unrelated to infringing use").

73. *Id.* at 1022. ("The record supports the district court's finding that Napster has actual knowledge that specific infringing material is available using its system, that it could block access to the system by suppliers of the infringing material, and that it failed to remove the material."). *Sony* also takes into consideration the ability to control. *Sony*, 464 U.S. at 436–38.

> In such cases, as in other situations in which the imposition of vicarious liability is manifestly just, the "contributory" infringer was in a position to control the use of copyrighted works by others and had authorized the use without permission from the copyright owner. This case, however, plainly does not fall in that category. The only contact between Sony and the users of the Betamax that is disclosed by this record occurred at the moment of sale.

Id.; *see also* RCA Records v. All-Fast Sys., Inc., 594 F. Supp. 335–39 (S.D.N.Y. 1984) (pointing out that manufacturers have no control over the use of a duplicating machine once it is sold).

74. Videocassette recorder ("VCR") manufacturers in *Sony* might have been held liable if manufacturers knew or should have known that any one of the VCR purchasers was engaged in infringing activity. *Sony*, 464 U.S. at 439.

ster therefore materially contributes to the infringing activity.[75]

C. Vicarious Liability

In the context of copyright law, vicarious liability extends beyond the employer/employee relationship to cases where the defendant "has the right and ability to supervise the infringing activity and also has a direct financial interest in such activities."[76] Therefore, the requirements for vicarious liability can be summarized by the following two prongs: (1) a financial interest; and (2) the right and ability to supervise.[77] The *Fonovisa, Inc. v. Cherry Auction Inc.*[78] opinion addressed the first prong by stating that financial interest exists where the availability of infringing material acts as "a 'draw' for customers." The panel found that such a situation existed because "Napster's future revenue [was] directly dependent upon 'increases in userbase.'"[79] As for the second prong, regarding the right to supervise, because Napster expressly reserved the right to refuse service and terminate accounts in its discretion, the panel agreed with the district court's finding that Napster retained the right to control access to its system.[80] Although the court found Napster's ability to supervise was limited by their system's architecture,[81] the court held Napster had at least an ability to locate infringing materials by file names, including those that reasonably or roughly correspond to the material contained in the listed contents.[82] Accordingly,

---

75. A & M Records, Inc. v. Napster, Inc., 114 F. Supp. 2d 896, 920 (N.D. Cal. 2000) (stating "without the support services defendant provides, Napster users could not find and download the music they want with the ease of which defendant boasts"); *see also Fonovisa*, 76 F.3d at 264; *Netcom*, 907 F. Supp. at 1374 ("Netcom will be liable for contributory infringement since its failure to cancel [a user's] infringing message and thereby stop an infringing copy from being distributed worldwide constitutes substantial participation.").

76. *Gershwin*, 443 F.2d at 1162; *see also* Polygram Int'l Publ'g, Inc. v. Nevada/TIG, Inc., 855 F. Supp. 1314, 1325–26 (D. Mass. 1994) (describing vicarious liability as a form of risk allocation).

77. *Fonovisa*, 76 F.3d at 262.

78. *Id.* at 263 (stating financial benefit may be shown "where infringing performances enhance the attractiveness of a venue").

79. A & M Records, Inc. v. Napster, Inc., 239 F.3d 1004, 1023 (9th Cir. 2001).

80. *Id.*

> Here, plaintiffs have demonstrated that Napster retains the right to control access to its system. Napster has an express reservation of rights policy, stating on its website that it expressly reserves the "right to refuse service and terminate accounts in [its] discretion, including, but not limited to, if Napster believes that user conduct violates applicable law . . . or for any reason in Napster's sole discretion, with or without cause."

Id.

81. *Id.* at 1024.

82. *Id.*

> Put differently, Napster's reserved "right and ability" to police is cabined by the

the panel held that "plaintiffs have demonstrated a likelihood of success on the merits of the vicarious copyright infringement claim."[83]

D. Scope of Preliminary Injunction

The *Napster IV* court concluded that the plaintiffs demonstrated a likelihood of success on the merits of both the contributory and vicarious infringement claims.[84] The panel determined, however, that the scope of the district court's preliminary injunction was overbroad.[85] On remand, the panel required that the district court modify the injunction to hold Napster liable for contributory copyright infringement

> [O]nly to the extent that Napster: (1) receives reasonable knowledge of specific infringing files with copyrighted musical compositions and sound recordings; (2) knows or should know that such files are available on the Napster system; and (3) fails to act to prevent viral distribution of the works . . . . Napster may be vicariously liable when it fails to affirmatively use its ability to patrol its system and preclude access to potentially infringing files listed in its search index.[86]

E. Safe Harbor Provisions

In *Napster I*, Napster argued that the DMCA's two safe harbor provisions apply to its allegedly infringing actions.[87] Napster first sought protection under the § 512(a) safe harbor provision for service providers who provide passive conduit functions.[88] The district court denied Napster's

---

system's current architecture. As shown by the record, the Napster system does not "read" the content of indexed files, other than to check that they are in the proper MP3 format. Napster, however, has the ability to locate infringing material listed on its search indices, and the right to terminate users' access to the system. The file name indices, therefore, are within the "premises" that Napster has the ability to police. We recognize that the files are user-named and may not match copyrighted material exactly (for example, the artist or song could be spelled wrong). For Napster to function effectively, however, file names must reasonably or roughly correspond to the material contained in the files, otherwise no user could ever locate any desired music. As a practical matter, Napster, its users and the record company plaintiffs have equal access to infringing material by employing Napster's "search function."

Id.

83. *Id.*

84. A & M Records, Inc. v. Napster, Inc., 239 F.3d 1004, 1019–29 (9th Cir. 2001).

85. *Id.* at 1027.

86. *Id.*

87. A & M Records, Inc. v. Napster, Inc., No. C 99-05183 MHP, 2000 U.S. Dist. LEXIS 6243, at *9–*12 (N.D. Cal. May 5, 2000).

88. *Id.* at 19; 17 U.S.C. § 512 (1994 & Supp. V 1999).

motion for summary judgment on this point.[89] The district court determined that Napster is not a passive conduit because the allegedly infringing material was passed between users, instead of through Napster's server.[90]

The court went on to recognize that whether Napster was eligible for the § 512(d) safe harbor provision for service providers who offer information location tools was an issue to be more fully developed at trial.[91] The *Napster IV* court affirmed the denial of Napster's summary judgment motion because the applicability of the safe harbor provisions still hinged upon several undecided questions, including

> (1) whether Napster is an Internet service provider as defined by 17 U.S.C. § 512(d); (2) whether copyright owners must give a service provider "official" notice of infringing activity in order for it to have knowledge or awareness of infringing activity on its system; and (3) whether Napster complies with § 512(i), which requires that a service provider to [sic] timely establish a detailed copyright compliance policy."[92]

Napster arguably should qualify under the § 512(d) safe harbor provision.[93] Napster's service has a searchable directory and index.[94] Furthermore, Napster representatives use the phrase "information location tool" to characterize some Napster functions.[95] It is likely that Napster will qualify as an "information location tool" under § 512(d).[96] Section 512(d) limits liability for situations where a service provider obtains knowledge by means of a notification procedure[97] and situations where a service provider obtains knowledge of infringing material or activity.[98] Nevertheless, it does not restrict the means by which copyright owners give "official" notice to service providers.[99]

---

89. A & M Records, Inc. v. Napster, Inc., No. C 99-05183 MHP, 2000 U.S. Dist. LEXIS 6243, *25 (N.D. Cal. May 5, 2000).

90. *Id.* at *23–*24.

91. *See id.* at *18–*19.

92. A & M Records, Inc. v. Napster, Inc., 239 F.3d 1004, 1025 (9th Cir. 2001).

93. *See* 17 U.S.C. § 512(d).

94. *Id.*

95. A & M Records, Inc. v. Napster, Inc., No. C 99-05183 MHP, 2000 U.S. Dist. LEXIS 6243, at *13–*15 (N.D. Cal. May, 5 2000).

96. *Id.* at *15–*16.

97. *Id.* at *18; 17 U.S.C. § 512(d)(3) (1994 & Supp. V 1999); *see also* Reply Brief for Appellant, at 29, Napster, Inc. v. A & M Records, Inc., 239 F.3d 1004 (9th Cir. 2001) (Nos. 00-16401 & 00-16403).

98. 17 U.S.C. § 512(d)(1)(c).

99. *Id.* § 512(d).

III. POST-NAPSTER: CENTRALIZED P2P AND DECENTRALIZED P2P

The post-Napster P2P systems that enable users to exchange digital content can be roughly divided into two categories: centralized and decentralized P2P networks.[100] Centralized P2P networks like Napster rely on one or more central servers.[101] This type of P2P network uses a central server for indexing file location information shared in the network.[102] The central server often serves additional functions such as providing chat room fora.[103] Once a user identifies the file location, the software enables the user's computer to download a requested file directly from the host computer.[104] Currently, many P2P service providers, including Napster, prefer this model for their systems because it permits the service providers to: (1) grant users access to the service provider's system and website; and (2) collect information about users' identities and their service use patterns.[105] Sponsors and advertisers have a great interest in both of these.[106]

Decentralized P2P networks, like Gnutella and its numerous software clones,[107] do not require a central server to index available content.[108] Instead, such networks enable users to obtain file location information and download content directly from other users in the network.[109] In a decentralized P2P network, individual users' computers pass information from computer to computer, relaying file inquiries and responses.[110] Once a file location is identified, the software enables a user's computer to request and download a file directly from the host computer containing the file.[111] As a result, no central server is necessary to index file locations.[112]

---

100. Howard Siegel & Benjamin Semel, *Strategy He Share, She Share: Sorting Out the State of Music File Swapping Online After Napster*, 18 E-COMMERCE LAW & STRATEGY 1 (July 2001), LEXIS, Secondary Legal, Legal Publications Group File.

101. *The P2P Myth*, *supra* note 34.

102. Chris Sherman, *NAPSTER: Copyright Killer or Distribution Hero?*, ONLINE, Nov. 2000, *available at* http://www.findarticles.com/cf_0/m1388/6_24/66456907/print.html.

103. *Id.*

104. *Id.*

105. *Id.*

106. *Id.*

107. *See The P2P Myth*, *supra* note 34.

108. *See* Sherman, *supra* note 102.

109. *Id.*

110. *Id.*

111. *Id.*

112. *Id.*

A. Liability of Post-Napster Centralized P2P Networks

1. Liability of Centralized P2P Networks

Centralized P2P networks are likely to be held liable for contributory and vicarious infringement under the precedent established by the *Napster* cases, because these services share similar critical features with Napster. Centralized P2P services may be found contributorily liable if the service provider gained knowledge, or had reason to know of, the availability of infringing material on the system.[113] Such services' centralized indices of file location information make it possible for service administrators to limit infringing activities by removing information from the index.[114] Thus, they materially contribute to any infringing activities by providing support services that enable users to find and download music with ease.[115] These services may be held vicariously liable because they usually have a financial interest arising from the maintenance of their userbases.[116] Moreover, they have a right to supervise because they usually set forth terms of service reserving rights to terminate a user's privileges.[117] Finally, centralized P2P networks also have the ability to supervise content to the extent that their central server provides the index of content.[118]

2. Variations on Centralized P2P Systems

Because of variations in the unique features that P2P services other than Napster provide, further analysis is necessary to determine these systems' ultimate copyright liability.

a. Napster-Compatible Clone Servers

Napster compatible centralized P2P systems are services that allow Napster users to access an independent Napster clone server, which in turn provides services identical to those provided by Napster's central server.[119] Napster users gain access to these clone servers by installing special client

113. A & M Records, Inc. v. Napster, Inc., 239 F.3d 1004, 1027 (9th Cir. 2001).

114. Sherman, *supra* note 102.

115. *See id.*

116. A & M Records, Inc. v. Napster, Inc., 239 F.3d 1004, 1023 (9th Cir. 2001).

117. *Id.* at 1023–24.

118. Lou Dolinar, *Napster Not Only Way to Swap a Song; Recording Firms Want Payment*, CHI. TRIB., Apr. 30, 2001, at Business 3, LEXIS, News.

119. *See OpenNap: Open Source Napster Server*, *at* http://opennap.sourceforge.net (last visited Oct. 6, 2001).

software in addition to Napster's MusicShare program.[120] These services emerged because Napster's server was overcrowded and concerns arose that content providers' legal threats would shut Napster down.[121] Because these clone servers work similarly to the Napster server,[122] the server operators may be held contributorily and vicariously liable under *Napster IV*.[123] These clone server operators are typically different from Napster in the following respects: (1) they piggyback on the Napster system by requiring users to install MusicShare and then add servers accessible through the Napster system (*i.e.*, users cannot operate the clone services without the Napster software);[124] (2) additional client software and server software for clone servers are not necessarily developed and distributed by clone server operators, unlike Napster's software.[125] However, these facts are likely of negligible significance in determining the Napster clones' liability because the indices of available copyrighted content they provide in the network is the essence of their contribution to the users' direct infringement.

Unique aspects of clone server operators give rise to questions as to whether they can be held vicariously liable for direct copyright infringement by their users. Because many of these servers are run by individuals, they may not necessarily have their own terms of service. This could mean that the individuals have not retained their rights to terminate if users are engaged in infringing conduct. In such cases, there is no "right to supervise" retained by the clone server operator, and, under *Napster IV*, no vicarious liability may be found.[126] However, because these clone servers are operated in conjunction with the Napster service, further assessment may be necessary to determine whether or not Napster's terms of service are applicable to services offered by clone server operators.

In addition, one element of the *Napster IV* ruling was partially based on the finding that Napster has a financial interest in keeping its user-base.[127] It is possible that the clone server operators do not keep a user-base. Furthermore, they could be operating clone servers for non-profit

120. *See, e.g.*, *Your Navigator to Internet Audio*, *at* http://www.napigator.com (last visited Oct. 19, 2001).

121. Charles Mann, *The Heavenly Jukebox; Efforts to Obtain Control Access to Sound Recordings from the Internet*, ATLANTIC MONTHLY, Sept. 1, 2000, at 39.

122. *See generally* Dave Wilby, *Top of the Swaps; Six Music Sharing Web Sites*, INTERNET MAG., Sept. 1, 2001, at 96.

123. *See* A & M Records, Inc. v. Napster, Inc., 239 F.3d 1004, 1023 (9th Cir. 2001).

124. *See, e.g.*, Gwendolyn Mariano, *Napster Upgrade Clips Same Clones*, CNET NEWS.COM (June 29, 2001), *at* http://news.cnet.com/news/0-1005-202-6416843.html.

125. *See OpenNap: Open Source Napster Server*, *at* http://opennap.sourceforge.net (last visited Oct. 6, 2001).

126. A & M Records, Inc. v. Napster, Inc., 239 F.3d 1004, 1023–24 (9th Cir. 2001).

127. *Id.* at 1023.

purposes, such as to promote information and content dissemination, because of a belief in making free information available on the Internet. In such cases, it may be difficult to find clone server operators vicariously liable. However, because running a server incurs costs, such as fees paid to Internet service providers ("ISPs"), most of the clone server operators likely have some commercial or economic justification for offering the service.

b. Independent Centralized P2P Networks

Centralized P2P networks that are similar to, but independent from Napster have a central server that indexes the available content, distributes client software to enable users to access their central server and share files directly with other users, and tends to have chat and instant messaging features like Napster.[128] Because they share features similar to Napster, this category of service may be held liable under *Napster IV* for contributory infringement and vicarious infringement if these service operators knew or had reason to know that the infringing copyrighted file sharing occurs within its system.[129]

c. Encrypted Centralized P2P Networks

Encrypted centralized P2P networks describes services that encrypt files and communications between their users.[130] With such a system, there is no way to know whether infringing activities are occurring within the network.[131] Although this feature does not affect the legal framework under which the *Napster* cases found centralized P2P networks liable, enforcement problems exist because decrypting the files in the network arguably can result in violations of the DMCA's anti-circumvention

128. *See Centralized File Sharing Networks: Others, at* http://www.infoanarchy.org/?op-special&page=centralized (last visited Sept. 10, 2001). For example, iMesh is one of the most popular Napster alternatives. *Napster Alternatives: The Best of the Rest, at* http://www.infoanarchy.org/?op=displaystory&sid=2001/3/6/215227/2776 (message posted by erik on Mar. 6, 2001). iMesh has multi-source downloading, but is a completely centralized network like Napster. *Id.* It reportedly installs "spyware," which silently transfers private information about its users to advertisers. *Id.* Another example of a Napster clone is Songspy. *Id.* Unlike the other programs mentioned, Songspy only shares MP3 files. *Id.*

129. A & M Records, Inc. v. Napster, Inc., 114 F. Supp. 2d 896, 918–19 (N.D. Cal. 2000).

130. *See* Lisa M. Bowman, *Aimster Fights Record Industry With Its Own Fuel*, CNET NEWS.COM (Mar. 2, 2001), *at* http://news.cnet.com/news/0-1005-20-5006958-0.html. For example, Filetopia has centralized file sharing features, chat, instant messaging, and catalog management. *Welcome to Filetopia, at* http://www.filetopia.org/home.htm (last visited Sept. 10, 2001).

131. *See* Bowman, *supra* note 130.

provisions.[132] Thus, content providers have no way to know whether the encrypted file contains copyrighted contents unless they circumvent the protection and decrypt it, which could violate the DMCA.[133] From this perspective, the DMCA may have a chilling effect and work against copyright owners.

d. Multiple Server Centralized P2P Networks

A centralized P2P system with multiple servers distributes both client and server software so that anyone can run their own server that functions similarly to the Napster server.[134] However, these servers route searches along the multiple server network in a Gnutella-like fashion.[135] Whether they utilize multiple servers or not, these services should be assessed under the same analysis applicable to Napster clone server operators.[136] As long as the servers index the file information or facilitate locating copyrighted contents in the network, the server operator can be held contributorily and vicariously liable under *Napster IV*.[137]

e. Centralized P2P Networks with "Spyware"

Centralized P2P systems with so-called "spyware"[138] are systems that secretly install additional software along with client P2P software on users' computers to enable the P2P service provider to collect information on users' use patterns and behaviors.[139] Some of these modules "silently transfer

132. *Id.*

133. *Id.* Aimster, a Napster clone, explicitly boasts that any attempt to decrypt the files may violate the DMCA. *Id.*

134. *See, e.g.*, *eDonkey 2000*, *at* http://www.edonkey2000.com/overview.html (last visited Oct. 13, 2001). These networks can also support multi-source downloading features. *See, e.g.*, *KaZaA—About Us*, *at* http://www.kazaa.com/index.php?page=about (last visited Sept. 20, 2001). KaZaA, based in Amsterdam, The Netherlands, reportedly plans to shift to a fee based service in the near future. *Zeropaid.com—KaZaA*, *at* http://www.zeropaid.com/kazaa (last visited Oct. 13, 2001). OpenNap can also be categorized as a multiple server system. *See* Siona LaFrance, *No Napster? No Problem*, NEWHOUSE NEWS SERVICE, Mar. 28, 2001, LEXIS, News Group File, All.

135. *See* Lisa Bowman, *Broadband Fans Busted over Gnutella*, CNET NEWS.COM (Apr. 17, 2001), *at* http://news.cnet.com/news10-1005-200-5641576.html [hereinafter *Busted over Gnutella*].

136. *See* discussion *supra* Part III.A.2.a.

137. *See* A & M Records, Inc. v. Napster, Inc., 239 F.3d 1004, 1019–24 (9th Cir. 2001).

138. *OptOut*, *at* http://www.grc.com/optout.htm (last visited Sept. 10, 2001).

139. *Net Speak*, COMPUTER WEEKLY, May 31, 2001, at 61. iMesh is reported to use spyware. *Centralized File Sharing Networks: Others*, *at* http://www.infoanarchy.org/?op-special&page=centralized (last visited Sept. 10, 2001); *see* John Borland, *"Spyware" Piggybacks on Napster Rivals*, CNET NEWS.COM (May 14, 2001), *at* http://news.cnet.com/news/0-1005-200-5921593.html.

private information" to sponsors and advertisers of the P2P system.[140] This feature arguably enhances the ability to police user behavior and increases the likelihood that such service providers will be held liable for vicarious infringement if they fail to police the infringing activity based on information acquired by spyware.

f. Centralized P2P Networks with File Identification Systems

Some centralized P2P networks have adopted file identification systems that allow file identification within the network by, for example, bit patterns or a unique identifier.[141] This system is designed primarily to enable multiple source downloads and/or resuming downloads.[142] When a download is requested, the central server searches its database for multiple copies of the same file based on this identification system.[143] This will enable the system to pull chunks of a requested file from multiple sources simultaneously, speeding up download times.[144] This identification system also can be used to "block out the transfer of copyrighted material."[145] This feature enhances the service provider's ability to control the flow of content because of file identification by content rather than file name.[146] Therefore, P2P systems with this kind of function can and must remove copyrighted content from their indices when they become aware of infringing activity in the network, regardless of file name misspellings.[147] Otherwise, they will likely be held contributorily liable.

---

140. *Napster Alternatives: The Best of the Rest*, *at* http://www.infoanarchy.org/?op=displaystory&sid=2001/3/6/215227/2776 (message posted by erik on Mar. 6, 2001).

141. Brian Copperman, *Search and Destroy, iMesh Goes Hunting*, *at* http://www.mp3.com/news/448.html (Nov. 19, 1999). For example, iMesh incorporates such a system. *Id.* iMesh also announced plans to build Digital Rights Management into its system. *Napster Alternatives: The Best of the Rest*, *at* http://www.infoanarchy.org/?op=displaystory&sid= 2001/3/6/215227/2776 (message posted by erik on Mar. 6, 2001). Carracho II's digital fingerprinting system has a similar function. *See* Leander Kahney, *Carracho II: Napster With a Plan*, WIRED NEWS (Feb. 17, 2001), *at* http://wired.com/news/technology/10,1282,41868,00.html.

142. *Using iMesh*, *at* http://www.imesh.com/using.html (last visited Oct. 13, 2001).

143. *Id.*

144. *Id.*

145. *Id.*

146. *See generally id.*

147. *See* Ben Charny & John Borland, *Is There Room on the Net for P2P?*, CNET NEWS.COM (Feb. 13, 2001), *at* http://news.cnet.com/news/0-1005-201-4810948-0.html [hereinafter *Is There Room on the Net for P2P?*].

g. File Sharing Requirements

Some P2P systems impose minimum sharing requirements before permitting a user to download from other users.[148] This is because the tendency of a small number of users is to share many files, while the vast majority of users share few. If such sharing policies are viewed as forcing users to share copyrighted materials, these features may create a higher likelihood of finding "material contribution" by the service provider—one factor for finding contributory infringement.

h. Foreign Central Server Locations

Some centralized P2Ps have central servers located outside the United States.[149] Whether these services are subject to jurisdiction of U.S. courts, whether they are liable under the U.S. Copyright Act, and the difficulties in enforcing the applicable laws, have placed these services last on the list of P2P services copyright holders are pursuing.[150] However, considering the rapid increase in Internet users throughout the world and the potential impact on the copyright holders' business, it will most likely not be long before copyright holders initiate legal action against such service providers.[151]

3. Applicability of Safe Harbor

None of the pure centralized P2P services transmit files through their central servers.[152] Therefore, it is unlikely that these centralized P2P services qualify for a safe harbor defense under section 512(a) of the DMCA.[153] However, centralized P2P services invariably provide file location information indices, which are likely to be deemed an "information lo-

148. *Napster Alternatives: The Best of the Rest*, *at* http://www.infoanarchy.org/?op=displaystory&sid=2001/3/6/215227/2776 (message posted by erik on Mar. 6, 2001). Some servers that run DirectConnect reportedly have this kind of requirement. *Id.* Also, Songspy adopted a "Karma policy," rewarding those users who share more. *Id.*

149. Copperman, *supra* note 141.

150. *See Is There Room on the Net for P2P?*, *supra* note 147.

151. *See id.*; *see also Napster Alternatives Start Blocking Songs*, *supra* note 14. The RIAA notified iMesh that it must make its users cease their infringing activities. *Id.* iMesh has announced that it will introduce copyright protection technology into its system. *Id.* A recent suit filed in California against post-Napster services names defendants in the West Indies and The Netherlands. *See* Complaint, MGM Studios Inc. v. Grokster, Ltd. (C.D. Cal. Oct. 2, 2001), *available at* http://www.riaa.org/pdf/complaint.pdf.

152. *See The P2P Myth*, *supra* note 34.

153. Fred von Lohmann, *Peer-to-Peer File Sharing and Copyright Law after Napster*, Electronic Frontier Foundation, *at* http://www.eff.org/IP/P2P/Napster/20010227_p2p_copyright_white_paper.html (2001).

cation tool."[154] Therefore, centralized P2P services are likely to qualify for a safe harbor defense under § 512(d) so long as they comply with the other requirements, such as maintaining a copyright compliance policy and quickly removing infringing information after notification from copyright owners.[155]

B. Liability of Decentralized P2P Networks—Gnutella and Others

1. Decentralized P2P Networks

Despite Napster's failure to overcome pressure from the Recording Industry Association of America ("RIAA"), many observe that Gnutella and some other P2P file sharing systems are likely to largely replace Napster and threaten content providers in the entertainment industry in the near future.[156] There are numerous so-called "cousins" of Gnutella.[157] The "cousins" share the same platform as Gnutella and can even share files of any type through the Gnutella network among those who use the Gnutella-based software.[158] They offer various competing features, however. For example, one offers a "resume" function that allows users to resume downloading from the point where the user aborted the download.[159] These decentralized P2P networks are depicted as "immune"[160] from copyright enforcement because they do not have central servers and merely consist of numerous individual users.[161] To enforce copyrights of digital content distributed by a decentralized P2P network, one feasible option for content providers is to target P2P software developers and distributors.[162] The motion picture and recording industries in fact announced a suit against post-Napster services on October 3, 2001.[163]

---

154. *See* A & M Records, Inc. v. Napster, Inc., 2000 U.S. Dist. LEXIS 6243, *1, *4, *16 (N.D. Cal. 2001).

155. 17 U.S.C. § 512(d) (1994 & Supp. V 1999).

156. Bowman, *supra* note 130.

157. *Napster Alternatives: The Best of the Rest*, *at* http://www.infoanarchy.org/?op=displaystory&sid=2001/3/6/215227/2776 (message posted by erik on Mar. 6, 2001).

158. *See id.*

159. Copperman, *supra* note 141.

160. *Is There Room on the Net for P2P?*, *supra* note 147.

161. Bowman, *supra* note 130. Of course, users are not immune from copyright infringement liability per se. *See* von Lohmann, *supra* note 153. However, there are difficulties in legal enforcement against individual users, and content providers may prefer not to pursue these users. *See* discussion *infra* Part V.

162. *See generally* von Lohmann, *supra* note 153 (discussing how P2P software developers, can reduce the chance of being sued by content providers and copyright owners).

163. Press Release, RIAA, Motion Picture and Recording Industries File Suit Against Music

Because the vast majority of users must install P2P file sharing software to gain access to the network, holding P2P software developers and distributors liable may stop infringement by P2P file sharing at its source. Software developers' liability in the context of decentralized P2P is not clear at the moment, but it seems unlikely that developers will be held liable under the *Napster* cases. It is difficult to hold such developers/distributors contributorily liable because: (1) there is usually no way of "knowing" when infringement occurs by users of P2P software;[164] and (2) there are doubts as to whether merely developing and providing software amounts to "material contribution."[165] It is also difficult to hold these developers/distributors vicariously liable because, generally: (1) they do not have the right[166] or the ability to supervise or police users' activities; and (2) they do not charge any fees nor keep any userbase.[167] In addition, even if decentralized P2P developers/distributors are found contributorily or vicariously liable, these developers/distributors may yet invoke the defense established by *Sony Corp. of America v. Universal City Studios, Inc.*[168] As discussed below, the *Sony* defense is available because even if the developers/distributors become aware of infringing uses, there is generally no way for them to prevent it.[169]

City and Others (Oct. 3, 2001), *at* http://www.riaa.org/PR_Story.cfm?id=456.

164. *See generally* von Lohmann, *supra* note 153 (explaining that after P2P developers receive notice that their systems are being used for infringing activity, they have a duty to stop it).

165. *But see id.* (explaining that in most instances "material contribution" has been met if the individual's system adds any value to an infringing user's experience).

166. However, clickwrap license agreements are likely to include termination policies. *See generally Music City*, *at* http://www.musiccity.com/policy.htm (last visited Oct. 6, 2001). Therefore, the right to terminate the license is reserved to the software distributor subject to validity of clickwrap agreements under contract law. *See generally* Daniel B. Ravicher, *Facilitating Collaborative Software Development: The Enforcability of Mass-Market Public Software Licenses*, 5 VA. J.L. & TECH 11, ¶ 85 (Fall 2000), *at* http://www.vjolt.net/vol5/issue3/v5i3a11-Ravicher.html.

167. *See* Riehl, *supra* note 169, at 1769, 1777.

168. 464 U.S. 417, 442–44 (1983). Although the *Napster IV* court found the *Sony* defense inapplicable to a vicarious liability claim, A & M Records, Inc. v. Napster Inc., 239 F.3d 1004, 1022 (9th Cir. 2001), that reasoning is not very persuasive given that the *Sony* Court affirmatively declined to distinguish vicarious liability from contributory liability. *See Sony*, 464 U.S. at 435 & n.17 (stating that "the concept of contributory infringement is merely a species of the broader [concept of vicarious liability,] necessarily entail[ing] consideration of arguments and case law which may also be forwarded under the other label[of vicarious liability]").

169. *See* Damien A. Riehl, *Electronic Commerce in the 21st Century: Article Peer-to-Peer Distribution Systems: Will Napster, Gnutella, and Freenet Create a Copyrighted Nirvana or Gehenna?*, 27 WM. MITCHELL L. REV. 1761, 1787 (2001).

2. Applicability of *Sony*

In *Universal City Studios, Inc. v. Sony Corp. of America*,[170] the Ninth Circuit concluded that, because virtually all television programming is copyrighted material, "videotape recorders are not 'suitable for substantial noninfringing use.'" Further, noting that "videotape recorders are manufactured, advertised, and sold for the primary purpose of reproducing television programming," the Ninth Circuit concluded that manufacturers and sellers were contributory infringers.[171] However, the Supreme Court applied a patent law doctrine relating to staple articles of commerce and concluded that manufacturers of videocassette recorders ("VCRs") and videocassette tapes were not contributory infringers because the VCRs and tapes had "substantial noninfringing uses."[172]

The *Napster IV* court held that *Sony's* "substantial noninfringing uses" defense is inapplicable where a system operator knows of actual infringement.[173] Unlike centralized P2P systems like Napster, a decentralized P2P system is likely to qualify for the *Sony* defense with regard to secondary infringement claims because software developers/distributors simply offer the software to users.[174] Once users gain access to the software, software developers/distributors generally have no means of "knowing" of infringement and no means to "control" or "supervise" users, even if notified of infringing activities.[175] A decentralized P2P software developer/distributor is arguably analogous to the VCR manufacturer/distributor in *Sony*. Therefore, although *NapsterIV* can be read to mean that contributory or vicarious infringers cannot resort to the *Sony* defense when they have knowledge of actual infringement, this does not apply to decentralized P2P developers/distributors.[176] Decentralized P2P developers/distributors qualify for the *Sony* defense, even if they become aware of actual infringement.[177]

---

170. 659 F.2d 963, 975 (9th Cir. 1981), *rev'd*, 464 U.S. 417 (1983) (quoting 3 MELVILLE B. NIMMER & DAVID NIMMER, NIMMER ON COPYRIGHT § 12.04[A] (1981)).

171. *Id.*

172. *Sony*, 464 U.S. at 442, 456.

173. A & M Records, Inc. v. Napster Inc., 239 F.3d 1004, 1020 (9th Cir. 2001).

174. *See Sony*, 464 U.S. at 435. The *Sony* defense applies to both contributory and vicarious infringement. *Id.*

175. *Id.*

176. *See* A & M Records, Inc. v. Napster, Inc., 239 F.3d 1004, 1020 (9th Cir. 2001).

177. *See* Blaine C. Kimrey, *Amateur Guitar Player's Lament II: A Critique of A&M Records, Inc. v. Napster, Inc., and a Clarion Call for Copyright Harmony in Cyberspace*, 20 REV. LITIG. 309, 327 (2001) (analyzing distinctions between *Sony* and the *Napster* cases).

Contributory infringement is generally divided into two categories: (1) personal conduct that encourages or assists the infringement; and (2) the contribution of machinery or goods that facilitates the infringement.[178] Whether a potential infringing act falls into one of these categories can be determined by asking whether the potential contributory infringer had the ability to either prevent further infringement or to correct the infringing situation.[179] Under the contribution of machinery/goods category, a provider will not be held liable as a contributory infringer if the equipment at issue has "substantial noninfringing uses."[180]

The *Napster IV* court, which did not apply *Sony* because of Napster's "knowledge,"[181] should be narrowly read and interpreted to apply specifically to the encouraging/assisting category. *Sony* does not apply to the encouraging/assisting category, where a potential contributory infringer has the ability to control the infringing situation.[182] Napster falls under this category.[183] However, under the provision of machinery/goods category, the provider should not be held liable even if the provider later became aware of the actual infringement by the users after the distribution of machinery/goods. It would be either overly burdensome or impossible for providers to prevent or correct the infringing situation because they lack the ability to control users' activities.[184] So long as there is a substantial noninfringing use of the machinery/goods at the time of distribution, providers should not be held contributorily liable for infringing use by the users. The exception would be if the machinery/goods provider knew of a user's specific intention to use the machinery or goods for an infringing activity at the time of delivery of the machinery or goods.[185] In such a case, the machinery/goods provider should be held liable for contributory infringement.[186]

---

178. 3 MELVILLE. B. NIMMER & DAVID NIMMER, NIMMER ON COPYRIGHT § 12.04 (2000).

179. *See Sony*, 464 U.S. at 437.

180. A & M Records, Inc. v. Napster, Inc., 239 F.3d 1004, 1020 (9th Cir. 2001) (quoting *Sony*, 464 U.S. at 442).

181. *See id.* (finding that "*Sony*'s holding [is] of limited assistance to Napster [given Napster's] actual, specific knowledge of direct infringement").

182. *See id.*

183. *Id.*

184. *See, e.g.*, Riehl, *supra* note 169, at 1787.

185. *Sony*, 464 U.S. at 439 (stating that if liability was to be imposed on the petitioners, the liability must rest on the fact that its customers may use that equipment to make unauthorized copies of copyrighted material).

186. *See* A & M Records, Inc. v. Abdallah, 948 F. Supp. 1449, 1460 (C.D. Cal. 1996). In this case, the defendant prepared "time-loaded" tapes timed to the specific length of the recording that users wished to counterfeit. *Id.* at 1453. The court rejected the applicability of *Sony* by ruling that there was no substantial noninfringing use of such tapes. *Id.* at 1456. In light of the sta-

Courts have found that a single potential noninfringing use is sufficient to qualify for the "substantial noninfringing uses" defense.[187] Decentralized P2P software is likely to be deemed to have a "substantial noninfringing use." Unlike VCRs, which inevitably cause reproduction of copyrighted material, P2P software can be used to share non-copyrighted material.[188] In fact, P2P systems are largely expected to become a major technological facilitator of exchange of information for academic research and business development on the Internet.[189]

3. Variations on Decentralized P2Ps

Gnutella is an open source protocol for decentralized P2P.[190] There is no official Gnutella-client software.[191] Therefore, various business models compete by featuring additional functions and features.[192] Some functions and features of these business models may give rise to additional issues worthy of consideration as to the liability of decentralized P2P and its users.

Closed decentralized P2P networks that utilize a file-sharing application allow businesses to bring employees together by enabling the exchange of information.[193] However, such networks also enable the exchange of copyrighted content as well.[194] Such networks are decentralized and also encrypted.[195] This kind of network raises the question of whether

---

ple article of commerce doctrine under patent law, the substantial noninfringing nature of machinery or goods should be judged individually. *See id.* The court made no clear distinction between "knowledge" and "substantial noninfringing use." *See id.* at 1456–57. Knowledge is about infringing activity or intention of the direct infringer, not about whether there is substantial noninfringing use of the machinery or goods. *Id.* at 1457.

187. *See* Vault Corp. v. Quaid Software Ltd., 847 F.2d 255, 266–67 (5th Cir. 1988); *see also* RCA/Ariola Int'l, Inc. v. Thomas & Grayston Co., 845 F.2d 773, 777, 781 (8th Cir. 1988).

188. For example, Freenet boasts that it enhances anonymous free speech by publishing articles in its network. Riehl, *supra* note 169, at 1779.

189. For example, DataSynapse contemplates using P2P architecture to link individual PCs into "a virtual supercomputer and harness unused processing power." *Is There Room on the Net for P2P?*, *supra* note 147.

190. Riehl, *supra* note 169, at 1776.

191. *Id.* at 1776–77.

192. *See, e.g.*, *Gnotella*, *at* http://www.gnotella.com (last visited Sept. 10, 2001); *BareShare*, *at* http://www.bareshare.com (last visited Sept. 6, 2001); *Limewire*, *at* http://www.limewire.com (last visited Sept. 6, 2001). Such features include search and response filtering, bandwidth regulation, multiple searches, skins, and private networks. *Id.*

193. *See Groove Networks*, *at* http://www.groove.net (last visited Oct. 23, 2001); *see Is There Room on the Net for P2P?*, *supra* note 147.

194. For example, Freenet focused its marketing campaign on copyright infringement aspects rather than the system's legitimate uses. *See* Riehl, *supra* note 169, at 1779–80.

195. *Id.*

sharing copyrighted materials among a limited number of users in a private group constitutes fair use under 17 U.S.C. § 107.[196] If such use within a small group is deemed fair use, it will be necessary to draw a line between closed P2P networks where such use is permissible and P2P networks where it is not.

As for enforcement of copyrights with respect to material exchanged over closed decentralized P2P networks with file sharing applications, it is technically difficult to detect infringing activity, if any, because of the encrypted and closed nature of the network.[197] If infringing activity is ever detected, network users are more likely than software developer/distributors to be an easy target for content providers. The limited number of users in the network may prompt content providers to sue the users as individuals, despite the decentralized nature of the system.

The incorporation of "spyware" into file-sharing programs allows the transmission of information regarding use of the P2P file-sharing program.[198] Spyware may become a hook to hold decentralized software developers/distributors liable under the *Napster* case because they have the means to know what their users are doing.[199] If the "ability to supervise" does not mean that the vicarious infringer must have means to locate and restrict the infringing activity, then merely having the ability to know of users' patterns and behavior may give rise to vicarious infringement if other requirements for liability are met. Because P2P software's terms of use usually include the service provider's right to terminate user licenses, a "right to supervise" is likely to be found. The collection of user information is clearly for establishing a "userbase," which will satisfy the financial interest requirement.[200] Therefore, if a decentralized P2P developer/distributor fails to police users' infringing activity, there is a possibility that such developer/distributor will be held vicariously liable.

---

196. *See* 17 U.S.C. § 107 (1994). "[U]se of a copyrighted work, including such use by reproduction in copies or phonorecords or by any other means specified by that section, for purposes such as criticism, comment, news reporting, teaching (including multiple copies for classroom use), scholarship or research, is not an infringement of copyright." *Id.*

197. Riehl, *supra* note 169, at 1783.

198. *See OptOut*, *at* http://grc.com/optout.htm (last visited Sept. 10, 2001); *see also BearShare*, *at* http://www.bearshare.com (last visited Sept. 10, 2001) (BearShare reportedly has spyware.); *Infoanarchy*, *at* http://www.infoanarchy.org/?op=special&page+gnutella (last visited Sept. 10, 2001).

199. *See* discussion *supra* Parts III.B.1~2.

200. *See* Fonovisa, Inc. v. Cherry Auction Inc., 76 F.3d 259, 262 (9th Cir. 1996) (quoting Gershwin Publ'g Corp. v. Columbia Artists Mgmt., Inc., 443 F.2d 1159, 1162 (2d Cir. 1971)).

4. Applicability of Safe Harbor

None of the DMCA's safe harbor provisions are applicable to decentralized P2P developers/distributors because they are not service providers.[201] The DMCA defines "service provider" as: (1) "an entity offering the transmission, routing, or providing of connections for digital online communications, between or among points specified by a user, of material of the user's choosing;" or (2) "a provider of online services or network access, or the operator of facilities."[202] This definition clearly intends to focus on online service providers, not software developers or distributors.[203] Further, developers and distributors have no ability to remove or disable access to the infringing materials.[204] Safe harbor provisions were provided because strict liability inevitably exposes Internet service providers to copyright infringement liability under the prescribed categories.[205] However, decentralized P2P software developers/distributors do not seem to fit into any of these categories. They merely develop and distribute software and do not offer information location services. Infringing material is never transmitted "through" their systems. They simply offer software for establishing independent networks over which users may exchange files.

IV. JAPAN: INTERNET INFRASTRUCTURE AND P2P

Delays in implementing effective measures to promote building broadband connection infrastructure caused Japan's development of the Internet to lag behind that of many developed countries.[206] However, rapid growth in xDSL[207] and the initiation of FTTH[208] services will likely enable Japanese net surfers to enjoy faster, convenient access to the Internet in

---

201. *See* 17 U.S.C. § 512(d) (Supp. V 1999); *see* A & M Records, Inc. v. Napster, Inc., 114 F. Supp. 2d 896, 919 (N.D. Cal. 2000).

202. 17 U.S.C. § 512(k)(1).

203. *Id.*

204. *See* Sherman, *supra* note 102.

205. *See* Kimrey, *supra* note 177, at 229–30.

206. *Korea Telecom Eyeing Japan's DSL Market*, ASIA PACIFIC TELECOM, June 1, 2001, at 11, LEXIS, News Group File, All.

207. "DSL (Digital Subscriber Line) is a technology for bringing high-bandwidth information to homes and small businesses over ordinary copper telephone lines." *Fast Guide to DSL*, *at* http://searchnetworking.techtarget.com/sdefinition/0,,sid7_gci213915,00.html (last visited Sept. 24, 2001). xDSL refers to different variations of DSL, such as ADSL, HDSL, and RADSL. *Id.*

208. Fiber to the home ("FTTH") service draws optical fiber directly to a user's home. *About DSL: FTTH*, *at* http://www.dslreports.com/information/kb/FTTH (last visited Sept. 18, 2001). Current service allows up to 100 megabytes-per-second connection speed to the Internet. *News Bursts*, ZDNET JAPAN, *at* http://zdnet.co.jp/news/bursts/0106/28/bflets.html (last modified June 28, 2001) (on file with author).

coming months.[209] A broadband connection to the Internet is a necessary condition for a P2P network to thrive.[210] However, the vast majority of Japanese Internet users still connect to the Internet by means of a dial-up connection.[211] Due to the inefficiency of downloading bulky files through the Internet, the online music distribution industry in Japan continues to stagnate.[212] The leading online music distribution site[213] estimates that it takes approximately seventeen minutes to download a four-minute song by means of a thirty-two kilobytes-per-second modem, which is the approximate average connection speed of Japanese users.[214] Downloading a CD containing several songs requires a user to patiently wait for as long as three hours.[215] Therefore, although Japan has been one of the top consuming countries of entertainment produced by the American entertainment industry, P2P file sharing has not yet become a major issue in Japan.[216] The potential of P2P networks is, however, one of the most noted topics among those who are aware of cutting-edge Internet technology.[217] One can easily

---

209. Currently, Japan is only fourth in the total number of page views per month in the world. *Internet Universe Grows by 6.8 Million Individuals in March*, Nielson Net Ratings, *at* http://www.eratings.com/news/20010430.htm (Apr. 30, 2001).

210. Alonso Quintana, Jay Ramsinghani & Tim Walls, *Peer-to-Peer Computing: The Search for Viable Business Models*, *in* KELLOGG TECHVENTURE 2001 ANTHOLOGY 10, *available at* http://www.ranjaygulati.com/teaching/tv2001/PEER-TO.pdf (last visited Sept. 18, 2001).

211. CSJ, Dai 13 kai CSJ WWW Riyosha Chosa Kekka [CSJ's Results of 13th Survey on Internet Users], *available at* http://www.csj.co.jp/www13/index.html (last visited Sept.15, 2001) (on file with author). Statistics show that over seventy percent of Internet users in Japan connect by means of dial-up, including modem and ISDN, which means that their connection speed can only be as high as sixty-four kilobytes-per-second. *Id.*

212. *See id.*

213. *Sony Bitmusic*, *at* http://bit.sonymusic.co.jp (last visited Sept. 18, 2001) (on file with author).

214. *See Survey Center*, *at* http://m1.channels.euroseek.com/662_E_5.html (last visited Oct. 13, 2001).

215. *See* Christopher Farley, *Finding His Voice: If You Want to Hear Folk-Rocker Ben Harper at His Best, Start Downloading*, TIME, Apr. 24, 2000, at 78, LEXIS, News Group Files, All.

216. It must be noted, however, that in June 2000, the Recording Industry Association of Japan ("RIAJ") submitted to Napster a list of copyrighted songs to block file sharing in Napster's system in accordance with the preliminary injunction. *RIAJ Asks Napster to Remove Songs*, *at* http://www.afterdawn.com/news/archive/2166.cfm (last visited Sept. 28, 2001).

217. Jun Murai, the president of the Japan Network Information Center ("JPNIC"), the sole organization in Japan that oversees international network resources such as domain names and Internet protocol ("IP") addresses, noted in a recent lecture to the effect that in the Internet society of the twenty-first century, P2P networks between and among mobile terminals that have global IP addresses will comprise the main character of the Internet rather than the traditional client/server system. Symposium, *The Internet Society in the 21st Century*, Japan Network Information Center, *available at* http://www.nic.ad.jp/jp/materials/symposium/20010316/20010316jpnic.pdf; *see also* Takuma Nakamura, *P2P as the Main Character in the 21st Century*, ZDNET NEWS JAPAN (Mar. 16, 2001), *at* http://www.zdnet.co.jp/news/0103/16/jpnic.html (on file

imagine that P2P technology will be in the hands of Japanese Internet users in the very near future, and inevitably, content providers will face issues concerning P2P file sharing before long.

In light of such concerns, this Part focuses on the potential liability under Japanese law of (1) centralized P2P services (*i.e.*, a hypothetical Japan-based version of Napster, hereinafter "J-Napster"); and (2) decentralized P2P networks (*i.e.*, a hypothetical Japan-based version of Gnutella, hereinafter "J-Gnutella").[218]

A. Napster in Japan

No case in the Japanese courts has addressed copyright infringement in connection with a P2P system comparable to Napster or Gnutella. In fact, not a single case involving the issue of unauthorized distribution of copyrighted content over the Internet has been decided.[219] Therefore, the following analysis is derived from theoretical possibilities, inferred from provisions of the Copyright Law of Japan ("CLJ")[220] and related copyright infringement cases.

If the *Napster* cases were litigated under CLJ, the conclusion would likely be similar to the U.S. decision, finding J-Napster and its users liable for copyright infringement. Sharing music files[221] widely among individu-

---

with author).

218. This proposed hypothetical is quite plausible. For example, iMesh, a comparative service based in Israel, currently has approximately twelve million members, a number that is expected to explode after the *Napster* decision. Jefferson Graham, *As Napster Shuts, Others Carry the Tune*, USA TODAY, July 12, 2001, *available at* http://www.usatoday.com/life/cyber/tech/2001-07-12-napster-usat-story.htm#more.

219. In Japan, the number of copyright infringement suits is steadily but gradually increasing. One-hundred seventeen such cases were brought in the year 1999. Supreme Court, *Chiteki Zaisan Kankei Minji Jiken no Ugoki* [*Status of Intellectual Property Related Case*], *at* http://courtdomino2.courts.go.jp/topics.nsf/ea145664a647510e492564680058cccc/d70944892813705b49256a760006356b?OpenDocument (last visited Nov. 13, 2001) (on file with author). In 1992, only sixty-six copyright cases were brought, the highest number achieved at that point. *Id.* Japanese culture has been tolerant of copyright infringement, in part because the country has been largely an importer of copyrighted works in the past centuries. *See generally* Yoshio Kumakura, *Quicker and Less Expensive Enforcements of Patents: Japanese Courts*, 5 CASRIP PUBLICATION SERIES: STREAMLINING INT'L INTELLECTUAL PROPERTY 31, 33 (1999) *at* http://www.law.washington.edu/casrip/symposium/number5/pub5atc15.pdf (details of statistics).

220. Chosakuken Ho [Copyright Law of Japan], Law No. 48 of 1970, translated at *Copyright Research and Information Center*, *at* http://www.cric.or.jp/cric_e/index.html (last visited Sept. 7, 2001) [hereinafter CLJ, Law No. 48 of 1970].

221. Under CLJ, "works" are granted the protection of the law. *Id.* "Work" means "a production in which thoughts or sentiments are expressed in a creative way and which falls within the literary, scientific, artistic or musical domain." *Id.* art. 2(1)(i). A song that consists of music and lyrics is generally protectable. *See id.* art. 2. Although phonograms that embody the performance by performers are not considered copyrightable works under the CLJ, "producers of

als is very likely to be deemed infringement of copyrights and neighboring rights, absent the success of the fair use defense, which is also unlikely to prevail. Unless any limitation of rights under the CLJ applies,[222] copying music data from a CD to a computer hard drive, and then copying from the hard drive to another user's hard drive via the Internet is considered "reproduction"[223] in this context.[224] Whether the copyright holder's exclusive right to make a performance "transmittable"[225] is infringed by making music files on users' hard drives transmittable is somewhat less clear. It appears the principle and spirit behind the right of making a performance transmittable is to give copyright owners control over when and how their work will be available to the on-line public. Therefore, there seems to be no strong justification to exclude the act of making copyrighted materials on users' hard drives transmittable from the scope of this right.[226] Accord-

---

phonograms" have the following neighboring rights: (1) "the exclusive right to reproduce their phonograms;" and (2) "the exclusive right to make their phonograms transmittable." *Id.* art. 96, 96*bis*. "Performers," on the other hand, have the following neighboring rights: (1) "the exclusive right to make sound or visual recordings;" and (2) "the exclusive right to make their performances transmittable." *Id.* art. 91(1), (2), 92*bis*(1).

222. *See* CLJ, Law No. 48 of 1970, *supra* note 220.

223. "Reproduction" means "the reproduction in a tangible form by means of printing, photography, polygraphy, sound or visual recording or otherwise." *Id.* art. 2(1)(xv).

224. Victor Entertainment K.K. v. Dailchi Kousho, 1057 Hanrei Times 221 (Tokyo Dist. Ct., May 16, 2000) (copying music data to a server constituted "reproduction" under the CLJ), *available at* http://www.softic.or.jp/eng/cases/STAR_Digioh10_17018.html. The same conclusion is also likely to be reached even if the conversion of the file format, *e.g.*, the conversion from wave format to MP3 format, occurs in the process of reproduction. *See* Hiroshi Saito, Chosakuken-hou [COPYRIGHT LAW], at 157 (Yuuhikaku 2000) (on file with author). It is not clear, however, who would be deemed the infringer: the user who allowed the copying of the file, the user who requested and received a copy of the file, or both.

225. *See* CLJ, Law No. 48 of 1970, *supra* note 220, art. 92*bis*(1). Owners of a copyright for a song, including performers and record producers, have exclusive rights to the interactive transmission of the music or lyrics, as well as the right to make the song transmittable. *See id.*; *see also id.* art. 2 (defining "public transmission," "interactive transmission," and "making [a work] transmittable").

226. The issue is whether any of these rights encompasses not only the act of uploading to a server, but also the requesting user's act of downloading directly from another user's hard drive. The majority of materials, including the language used in the English translation of the provision in question, suggests that the legislature primarily was concerned with servers, not with end users. Chosakuken-Hou/Fuseikyousou-Boushi-Hou Kaisei Kaisetsu—LEGAL PROTECTION OF DIGITAL CONTENTS [Annotation of Amendments to Copyright Law and Unfair Competition Law] at 64, 69, 73 (Chosakuken Hourei Kenkyukai & Chitekizaisan Seisaku Shitsu eds., Yuuhikaku 1999) (on file with author). From the plain language of the code, however, the general meaning of "making [a work] transmittable" can be interpreted to include copies resident on personal computers. *See* Takashi Yamamoto, *Napster Sosho Kousosin Hanketsu* [Appellate court decision in Napster litigation], The Record Ex-Number, '01 Vol.11, at 12 (2001) (on file with author). Certain P2P software also raises a related issue. Imagine P2P software that has a function that can restrict automatic copying of the files contained in the host user's personal computer. If such a function is activated, the host user is asked whether or not the host user will allow copying of the

ingly, by enabling other users to have access to files on a computer's hard drive by means of a connection to the Internet, without the copyright owner's authorization, such users infringe upon the CLJ right of reproduction and/or the right of making a work transmittable.[227]

The CLJ does not have a general fair use provision.[228] Instead, it has an enumerated list of exempted uses.[229] For example, reproduction for private use is permissible if the purpose of reproduction is for a limited circle, *e.g.*, for personal use or family use.[230] Although there is no precedent on this issue, reproduction of music files[231] for sharing with anonymous users over the Internet seems to clearly exceed such purpose and, therefore, the private use defense is likely to fail.[232]

B. Liability of J-Napster

There is no precedent that directly aids in predicting the outcome of a suit against J-Napster for copyright infringement.[233] However, copyright infringement claims in Japan are considered one category under general

---

user's file whenever requested by other users in the network. Should "making [a work] transmittable" only include those transmittable statuses where transmissions are initiated by automatic response to requests, there is a possibility that use of this kind of P2P software does not constitute infringement of the right to make a work transmittable if the law is interpreted strictly verbatim. *See* CLJ, Law No. 48 of 1970, *supra* note 220, art. 2(1)(ix*quinquies*).

227. Although there are some contrary opinions among scholars, the distribution right under the CLJ is generally understood to refer to a transfer of ownership of a work that is fixed in a tangible form. CLJ, Law No. 48 of 1970, *supra* note 220, art. 26*bis*(1); *see* Hiroshi Saito, Chosakuken Ho [Copyright Law of Japan], at 157 (Yuuhikaku 2000) (on file with author). Therefore, it is unlikely that infringement of the copyright holder's distribution right would be found in this situation.

228. *See* CLJ, Law No. 48 of 1970, *supra* note 220.

229. *Id.* art. 30–50. Although there is no Supreme Court case on this issue, it is generally understood that the list is exhaustive and that the CLJ does not allow exemptions other than those listed. *See* Takashi B. Yamamoto, *Copyright Protection of Databases: The Wall Street Journal Case, at* http://www.cric.or.jp/cric_e/cuj/cuj98/cuj98_2.html (last visted Nov. 2, 2001); *see also* Dow Jones & Co., Inc. v. Kabushiki Kaisha Knowhow Japan, 1524 Hanrei Jiho 118 (Tokyo High Court, Oct. 27, 1994) (on file with author).

230. *See* CLJ, Law No. 48 of 1970, *supra* note 220, art. 30(1).

231. This term's scope includes both reproduction from CD to hard drive and reproduction from a hard drive to another user's hard drive. *See* Hiroshi Saito, Chosakuken Ho [Copyright Law of Japan], at 157 (Yuuhikaku 2000) (on file with author). Transitory storage of files in random access memory is not considered reproduction. *Cf.* Fumio Sakka, *Changes in Japanese Society in the Course of Reform of the Copyright System: Centennial of the Copyright Law in Japan, available at* http://cric.or.jp.cric_e/cuj/cuj99/cuj99_1_4.html (last visited Oct. 13, 2001).

232. If, subsequent to the private use, the user distributed or made the copy available to the public, this would infringe upon the reproduction rights of the copyright owner. CLJ, Law No. 48 of 1970, *supra* note 220 (granting exclusive rights of reproduction to the copyright owner, except for the enumerated permissible uses, including personal use).

233. *See* discussion *supra* Part IV.A.

tort claims theory.[234] Therefore, tort cases not related to copyright infringements can also be of assistance in analyzing the J-Napster hypothetical case.

Neither the CLJ nor Japanese tort law provides a precedent concerning a service provider's liability in connection with copyright infringement by a third-party user.[235] A leading case, however, addressed service providers' liability in connection with third party defamatory conduct, the category of which is similarly analyzed under tort law.[236] In the famous case of *Nifty Serve K.K.*,[237] the Tokyo District Court held that a system operator for a personal computer network could be liable if: (1) the operator became aware of a defamatory statement posted on the forum; and (2) the operator failed to take necessary measures to prevent an individual from being defamed.[238] The court found that the system operator's duty to take such measures arose from duties in the general law regarding the maintenance of public order.[239]

In the subsequent case of *Toritsu Daigaku*,[240] the court denied a claim that a network administrator had an affirmative duty to delete a defamatory statement from a homepage built within the university's network.[241] The court held that the network administrator was not liable for merely recognizing the alleged defamatory statement on the system.[242] It is clear that Japanese courts address the liability of service providers in the context of the circumstances surrounding the service provider's possible duty to act.[243] Thus, Japanese courts have found the existence of a duty under general tort theory.[244] Correspondingly, this analysis could be applied to determine the

234. Katsunari Goto, *"Indirect Infringement" of Copyrights in a Multimedia Society*, *at* http://www.cric.or.jp/cric_e/cuj/cuj98/_4.html (last visited Sept. 18, 2001). The requirements for tort liability are: (1) illegal conduct in violation of a duty of care; (2) damages; (3) causation; and (4) negligence or willful intention. *See* Minpo [Civil Code of Japan], Law No. 89 of 1896, *amended by* Law. No. 41 of 2001, art. 709 [hereinafter Minpo].

235. *See* discussion *supra* Part IV.A.

236. [Undisclosed Party] v. Nifty Serve K.K., 1610 Hanrei Jiho 22 (Tokyo Dist. Ct., May 26, 1997) (on file with author).

237. *Id.*

238. *Id.*

239. *Id.* The service provider, Nifty Serve, subcontracted the administration of the forum to the system operator. *Id.* The court held Nifty Serve liable under an employer liability theory. *Id.*; Minpo, *supra* note 234, art. 715.

240. [Undisclosed party] v. Toritsu Daigaku [Toritsu University], 1707 Hanrei Jiho 139 (Tokyo Dist. Ct., Sept. 24, 1999) (on file with author).

241. *Id.*

242. *Id.*

243. *See generally id.*; *Nifty Serve K.K.*, 1610 Hanrei Jiho 22.

244. *See generally Nifty Serve K.K.*, 1610 Hanrei Jiho 22; *Toritsu Daigaku*, 1707 Hanrei Jiho 139.

liability of a direct infringer.

In December 2000, the First Sub-Committee of the Copyright Council (the "Committee")[245] published a report that included the Committee's analysis of the liability of Internet service providers (the "Report").[246] In the Report, the Committee proposed a framework for legislation setting forth service providers liabilities, which incorporated the decision reached in *Nifty Serve* and *Toritsu Daigaku*.[247] The proposed legislation divides potential liabilities into three categories: (1) when a service provider has affirmatively (and knowingly) been involved in unauthorized uploading of copyrighted work ("Category One"); (2) when a service provider was not involved in an infringing activity at the time of the uploading but later became or should have become aware of infringement and facilitated, assisted, or abandoned the infringing situation ("Category Two"); and (3) when a service provider was not involved in an infringing activity at the time of the uploading and did not know of the infringement, or there was a justifiable reason for not knowing the infringement, or the service provider lacked the technology to control the ability to infringe by deleting the unauthorized copy from the server or by other means ("Category Three").[248]

The Report suggests that service providers in Category One and Category Two may at least be subject to liability for monetary damages, but only service providers in Category One may be subject to claims for injunctive relief.[249] The reasoning behind this division is that service providers in Category Two did not engage in direct infringement by uploading, but merely made it possible for the transmitter (user) to infringe.[250] As for Category Three, the Report suggests that their service providers are not and cannot be held liable for monetary damages, nor subject to injunction claims.[251]

---

245. The Ministry of Education, Culture, Sports, Science and Technology established the Committee. *See ISP Responsibility Eyed for Piracy on Internet*, DAILY YOMIURI, Dec. 16, 2000, *available at* 2000 WL 30665836 [hereinafter *ISP Responsibility*]. Because the CLJ has been proposed and amended under the initiative of the Ministry, the Report is likely to have significant effect on the future legislation on these issues, if any. *Id.*

246. Shingi no Matome [Summary of Discussion] (Dec. 2000), *available at* http://www.mext.go.jp/b_menu/shingi/12/chosaku/toushin/001246.html [hereinafter *The Report*]; *see also ISP Responsibility*, *supra* note 245.

247. *See id.*; *see also Nifty Serve K.K.*, 1610 Hanrei Jiho 22; *Toritsu Daigaku*, 1707 Hanrei Jiho 139.

248. *The Report*, *supra* note 246; *see also ISP Responsibility*, *supra* note 245.

249. *See generally id.*

250. *See generally id.*

251. *See generally id.* Unlike the strict liability rule under the U.S. Copyright Act, the CLJ requires negligence to hold an infringer liable. 2 JAPAN INTERNATIONAL COPYRIGHT LAW AND PRACTICE § 8 (Matthew Bender & Co. 2000), *available at* LEXIS, All Sources, Country & Region (excluding U.S.), Japan, Commentaries and Treatises, International Copyright Law and

Although copyright infringement and the liability of service providers will likely be determined on a case-by-case basis under the tort theory,[252] the Report's analyses and conclusions are well founded in existing Japanese legal principles,[253] and are therefore likely to be the framework for assessing the liability of service providers.

Based on the CLJ Report's framework, J-Napster would likely be held liable if it became aware of, or had reason to know of, the infringing conduct of its users, and subsequently failed to prevent infringement by deleting copyrighted material from its central server index.[254] Category One would not likely apply to J-Napster because this category assumes that the service provider knowingly uploaded infringing materials to its own server.[255] Nor would Category Three apply to centralized P2P services like J-Napster because centralized P2P systems usually retain technological and contractual control over termination of service to users who wish to upload information to its central server.[256] On the other hand, J-Napster would likely be deemed to have facilitated, assisted, or abandoned the infringing situation under Category Two of the proposed framework.[257]

C. Liability of J-Gnutella

The governmental agency in charge of copyright law administration recognizes the concerns involving decentralized P2P networks like Gnutella.[258] However, there has been very little discussion regarding how to treat the widespread dissemination of digitized contents over the Internet using a decentralized P2P network.

Hypothetically, under the framework suggested by the Report, a J-Gnutella developer/distributor would not be liable for copyright infringement because such a developer/distributor would not have the technological

---

Practices. In addition, the Report upholds the principle that service providers should not be required to affirmatively police their servers for infringement. *The Report*, *supra* note 246; *see also ISP Responsibility*, *supra* note 245. Therefore, unless service providers become aware or neglect to become aware of infringing activity, service providers will never be held liable. *See id.* Based on these conclusions drawn from general tort law principles, which cover copyright infringement, it is possible to argue that Japan will never need to construct safe harbor provisions comparable to those contained in the DMCA. *See* 17 U.S.C. § 512 (1994 & Supp. V 1999).

252. *See generally Nifty Serve K.K.*, 1610 Hanrei Jiho 22; *Toritsu Daigaku*, 1707 Hanrei Jiho 139.

253. *Compare ISP Responsibility*, *supra* note 245, *with Nifty Serve K.K.*, 1610 Hanrei Jiho 22; *Toritsu Dangaku*, 1707 Hanrei Jiho 139.

254. *See generally ISP Responsibility*, *supra* note 245.

255. *See generally id.*

256. *See generally id.*

257. *See generally id.*

258. *See supra* text accompanying note 246.

capability to control its users' infringements.[259] Thus, a J-Gnutella developer/distributor would fall under Category Three of the Committee's proposed framework.[260] As previously discussed, decentralized P2Ps with quasi-centralized aspects could be analyzed under the centralized P2P liability theory set forth in the J-Napster hypothetical.[261]

Recently, Japan's Supreme Court issued an important decision on the liability of non-direct copyright infringers.[262] In this case, the court found that a commercial karaoke equipment leasing merchant had a duty to affirmatively confirm with the lessee, the karaoke bar operator, that the lessee was in compliance with applicable copyright law.[263] This duty required confirmation that, prior to delivery of the equipment to the lessee, the lessee had concluded or applied for copyright licensing agreements with the copyright owners of the songs to be played or displayed on the karaoke equipment.[264] However, the lessor failed to ensure that the lessee actually secured the copyright agreements; thus the court held the lessor liable for copyright infringement.[265] In this case, the lessor notified the lessee in writing and explained in advance the need for the lessee to sign copyright licensing agreements with copyright owners prior to operating the karaoke equipment.[266]

The Japanese Supreme Court held that the lessor's duty of care was based on the following reasons: (1) because a majority of the songs played or displayed by karaoke equipment is subject to copyright, karaoke equipment has a high possibility of facilitating copyright infringement unless the lessee obtains proper authorization; (2) copyright infringement is subject to criminal penalty; (3) the lessor gains commercial benefits by leasing this karaoke equipment; (4) because it is generally known that a large percentage of karaoke bar operators do not obtain copyright licensing agreements, the lessor should have foreseen the possibility of copyright infringement unless the lessor confirmed that the bar operators had obtained or applied for a copyright licensing agreement; and, finally (5) the lessor could easily confirm the existence of copyright license agreements and would therefore be able to implement measures to prevent copyright infringement.[267]

---

259. *The Report*, *supra* note 246; *see also ISP Responsibility*, *supra* note 245.

260. *See id.*

261. *See* discussion *supra* Part IV.B.

262. Japanese Society for Rights of Authors, Composers, and Publishers v. Yugen Kaisha Videomates, 1722 Hanrei Jiho 108 (Supreme Court, Mar. 2, 2001) (on file with author).

263. *Id.*

264. *Id.*

265. *Id.*

266. *Id.*

267. *Id.*

In its ruling, the Japanese Supreme Court vacated the lower court's decision that held that if the lessor notified the lessee in writing and explained the need for copyright license agreements upon signing the lease, the lessor had no further duty to confirm the lessee's compliance with copyright law.[268] The lower court's exception to this rule provided that only under special circumstances, such as when a lessee does not intend to obtain copyright licensing agreements, does the lessor have an affirmative duty to confirm with the lessee that these agreements have been concluded or requested from the copyright owner prior to delivery of the equipment.[269]

However, while this Japanese Supreme Court decision does not directly apply to P2P network operators and system developers, this case shows the court's strong policy to hold anyone liable who: (1) offers for profit equipment that has a high possibility of use requiring copyright owners' permission or otherwise facilitating copyright infringement; and (2) fails to take affirmative precautionary measures to prevent such copyright infringement.[270]

J-Gnutella's software enables users to locate copyrighted content and facilitates access to infringing content between users' hard drives.[271] If the spirit of the Japanese Supreme Court decision is honored, software developers/distributors have an affirmative duty to ensure that the software is not used for infringing activities given that such software has a high potential for profit-making infringing activities. Applying the Japanese Supreme Court decision, a Japanese court may justifiably impose an affirmative duty upon P2P software developers/distributors to: (1) warn respective users not to use the software for infringing purposes; and (2) reject software licensing unless the users affirmatively agreed not to use the software for infringing activities.[272] Thus, if the P2P software developers/distributors breach this duty, the court arguably may impose copyright infringement liability.

If courts impose this affirmative duty on developers/distributors, the details of the duty will depend on the features of the software and its means of distribution.[273] However, these duties will be limited to the extent that

---

268. Japanese Society for Rights of Authors, Composers, and Publishers v. Yugen Kaisha Videomates, 1722 Hanrei Jiho 108 (Supreme Court, Mar. 2, 2001) (on file with author).

269. Japanese Society for Rights of Authors, Composers, and Publishers v. Yugen Kaisha Videomates, Heisei 11nen (*ne*) 2788 [docket number 2788 of year 1999] (Tokyo High Court, Nov. 29, 1999) (on file author).

270. Japanese Society for Rights of Authors, Composers, and Publishers v. Yugen Kaisha Videomates, 1722 Hanrei Jiho 108 (Supreme Court, Mar. 2, 2001) (on file with author).

271. *The P2P Myth*, *supra* note 34.

272. *See id.*

273. *See id.*

performance does not excessively burden the software developer/distributor.[274]

D. Safe Harbor Provisions

Japan has no safe harbor provision that deals with the liabilities of Internet service providers. The Report concluded that Japan should seriously consider implementing legislation concerning the legal liabilities of Internet service providers in the context of copyright infringement.[275] However, because general tort law principles address copyright infringement, Japan may not need safe harbor provisions.

Nevertheless, the Report focuses on Internet service providers falling within Category Two because their affirmative duty, once aware of infringement, is somewhat unclear.[276] Indeed, the details of the Internet service providers' duty may depend on the circumstances of each individual case.[277] Therefore, the Report emphasizes the importance of further assessment and development of this proposed "notice and take down" policy to balance: (1) acts for which service providers should be liable; and (2) the undue burdens of determining whether an activity infringes.[278] The Report's proposed policy does not require Internet service providers to take down infringing material until they are notified under the formal "notice and take down" procedure.[279]

Following the Report's framework, it is highly unlikely that a centralized P2P network such as J-Napster would qualify under the proposed "notice and take down" procedure if it facilitated, assisted, or abandoned the infringement after it became aware or should have known of the infringement.[280] However, if J-Napster were notified of copyright infringement under the proposed "notice and take down" policy, it would likely be exempted from liability for copyright infringement so long as it has followed the policy appropriately.[281] As for decentralized P2P software developer/distributors such as J-Gnutella, it is clear that this safe harbor provision will not apply because it would not be deemed a service provider and

274. *See id.* For example, it is conceivable that a Japanese court may rule in the future that a clickwrap license agreement for P2P software must include provisions warning users and prohibiting them from engaging in infringing activities.

275. *ISP Responsibility*, *supra* note 245.

276. *See id.*

277. *Id.*

278. *Id.*

279. *Id.*

280. *See id.*

281. *See ISP Responsibility*, *supra* note 245.

it lacks a central server that exercises control over the infringing activity.[282]

V. FROM LEGAL ENFORCEMENT TO ENFORCEMENT BY DIGITAL TECHNOLOGY

A. Difficulty in Legal Enforcement

Although entertainment industry plaintiffs gained their first victory against Napster, they have not won their war.[283] The actual impact of the *Napster V* Order is quickly failing to meet expectations.[284] Immediately after the court issued the Order, Napster immediately announced that it had taken technological measures to filter the songs whose song titles, artist names and file names had been provided by copyright owners.[285] However, the filtering screen initially launched "easily allow[ed] misspelled files to slip through."[286]

Despite the fact that Napster has purchased its own staff to look for variations in spelling, access to a vast database of common song misspellings, and its own automated filter looking for likely misspellings or other filter-avoiding tricks, the presiding judge nonetheless characterized Napster's filtering efforts as "disgraceful" in light of plaintiffs' criticisms.[287] As a result, Napster temporarily suspended the file transfers.[288]

In addition, there are countless obstacles to the legal enforcement of copyrights in the P2P system: (1) in the case of centralized P2Ps, the effectiveness of filtering copyrighted content is still vulnerable so long as content providers and the P2P service providers rely on file names, song titles, and artist names;[289] (2) as for decentralized P2Ps, because there is no cen-

---

282. *See id.*

283. John Borland, *Judge Lets Napster Live Despite Injunction*, CNET NEWS.COM (Mar. 6, 2001), *at* http://news.cnet.com/news/0-1005-200-5039135.html [hereinafter *Judge Lets Napster Live*].

284. *Id.*

285. *Id.*

286. *Id.*

287. John Borland, *Judge: Napster Filtering Efforts "Disgraceful,"* CNET NEWS.COM (Apr. 10, 2001), *at* http://news.cnet.com/news/0-1005-200-5567384.html?tag=prntfr [hereinafter *Napster Filtering Efforts Disgraceful*]. As of the end of March 2001, Napster has blocked 311,000 individual works, although the RIAA reports that record labels have identified more than 600,000 songs. *Id.*

288. *Q&A on Temporary Suspension of File Transfers*, *at* http://www.napster.com/pressroom/010702-qanda.html (last visited Nov. 2, 2001).

289. *See Judge Lets Napster Live*, *supra* note 283. Programs once freely available on the Internet, such as Aimster, may be used to convert filenames into Pig-Latin or other codes to evade detection under the Order. *See, e.g.*, *Aimster Download*, http://www.aimster.com/

tral service provider to sue, content providers may be forced to enforce copyrights against individual users;[290] (3) even if a suit against decentralized P2P users individually was successful, the damages recoverable from each individual would be nominal, *e.g.*, the price of a CD multiplied by the number of copies distributed, plus fees and costs;[291] (4) even if record companies could obtain judgment in a substantial amount, the individual defendants might not have to pay for the damages if they simply declare bankruptcy;[292] (5) as there are millions of Napster users in the world, record companies may be required to file thousands of lawsuits to recover the majority of losses they have allegedly suffered;[293] (6) even if record companies only seek injunctions, it would still be technically difficult to locate the infringing individuals under the current P2P system;[294] (7) even if decentralized P2P software developers/distributors can be held liable for copyright infringement under the current law and even if content providers are able to stop distribution of such software, alternatives may emerge without difficulties because the Gnutella platform is an open source project like Linux;[295] (8) the picture of big conglomerates versus small individuals, many of whom are likely to be students, may create negative publicity for

---

pigencoder.phtml (last visited Sept. 14, 2001). Aimster ceased offering this capability on March 13, 2001. *Id.*

290. *See The P2P Myth*, *supra* note 34.

291. Michael B. Rutner, *The ASCAP Licensing Model and the Internet: A Potential Solution to High-Tech Copyright Infringement*, 39 B.C. L. REV. 1061, 1070 (1998), LEXIS, Law Reviews, Combined.

292. *E.g.*, Jim Oliphant, *Abortion Foes Cry Fiscal Foul*, LEGAL TIMES, Feb. 7, 2000, at 14, LEXIS, News Group File, Most Recent Two Years (illustrating the use of declaring bankruptcy to thwart paying judgments).

293. *See* John Borland, *Who Will Serve As Napster Police?*, CNET NEWS.COM (Mar. 27, 2001), *at* http://www.zdnet.com/zdnn/stories/news/0,4586,5080218,00.html [hereinafter *Napster Police*].

294. *See The P2P Myth*, *supra* note 34. Current technology is able to locate users through their IP addresses, which are exposed to a central server and other users when connecting to a P2P network. *Id.* Further concerns arise when the shared content is encrypted as in Freenet and Filetopia and content providers are unable to track what is being shared. *See* Hisamichi Okamura, *MP3 and Copyright (MP3 to Chosakuken-hou)*, *at* http://www.law.co.jp/okamura/copylaw/MP3.htm (last visited Nov. 2, 2001) (on file with author). Freenet is a type of network that aims to give publishers and readers anonymity; instead of allowing automatic download from their hard drives, users upload files they find interesting to the network. *See Freenet: What Is Freenet?*, *at* http://freenet.sourceforge.net/index.php?page=whatis (last visited Nov. 1, 2001). Those files are encrypted and divided into anonymous particles of files, which are then stored in a data haven on continuously changing user computer hard drives. *Id.* Even the computer owner does not know what is stored in his or her own hard drives. *See id.* Therefore, it is extremely difficult to locate who is infringing and what copyrighted works have been unlawfully distributed and reproduced.

295. *See The P2P Myth*, *supra* note 34.

record companies.[296]

Clearly, content providers will inevitably face challenges enforcing copyrights extraterritorially,[297] overcoming complicated issues concerning jurisdiction, choice of law and enforcement in other jurisdictions. The widespread use and operation of Napster and post-Napster services internationally makes such challenges likely to become a reality.[298]

B. Move from Legal Enforcement to Enforcement by Digital Technology

Approximately 2.7 billion songs were traded through the Napster service in February 2001 alone.[299] Damages for such infringement can total as much as $150,000 per song.[300] While the number of visitors in March 2001 dropped slightly to 15.7 million visitors from 16.9 million in February 2001, unique visits to the Napster service rose "from 5.9 million in February 2001 to 8.2 million in March 2001."[301] Thus, it is a daunting task for content providers to take appropriate and effective measures to ensure that the public does not illegally exploit their copyrights using P2P networks. Given the difficulties in legal enforcement, the most practical way to solve problems that were spawned by digital technology may be to utilize digital technology itself to solve the problem.

1. Technological Protection and Licensing

One way of securing copyrights in this context is by affording technological protection to digital contents. By affording protection to distributed digital contents, tangible or intangible, content providers can prevent users from freely transforming and distributing digital contents over the Inter-

---

296. *See* Jesse Feder, Symposium, *Fair Use, Public Domain or Piracy...Should the Digital Exchange of Copyrighted Works Be Permitted or Prevented?*, 11 FORDHAM INTELL. PROP., MEDIA & ENT. L.J. 265, 270 (Keynote Address 2001) ("If we have our law structured so that the only way a copyright owner can vindicate his rights is to go after individual end-users, we have lost the fight.").

297. *See id.*

298. *See Napster Police*, *supra* note 293. A recent suit filed in California against post-Napster services names defendants in the West Indies and The Netherlands. *See* Complaint, MGM Studios Inc. v. Grokster, Ltd. (C.D. Cal. Oct. 2, 2001), *available at* http://www.riaa.org/pdf/complaint.pdf.

299. John Borland, *Napster Filters More Than Half of Downloads*, CNET NEWS.COM (Mar. 15, 2001), *at* http://news.cnet.com/news/0-1005-200-5149337.html.

300. *Judge Lets Napster Live*, *supra* note 283.

301. Melanie Austria Farmer, *Napster Traffic Slows in U.S.*, CNET NEWS.COM (Apr. 13, 2001), *at* http://news.cnet.com/news/0-1005-200-5593639.html. Unique visits are visits by one person counted only once per month. *Id.*

net.[302] The entertainment industry does recognize the importance of this measure and did not delay in asking the courts and the legislature to help it.[303] One of the ways to afford such protection is to encrypt music or song data on CDs so that users cannot "rip" or encode them into MP3 files for distribution.[304] Because of the concern that encryption of data on CDs may make them unplayable on some CD players already in the market (which definitely will offend consumers), record companies were reluctant to introduce encryption to CDs.[305] However, a recent report revealed that the first encrypted CDs are about to be released, while major labels are currently evaluating encryption technology for CDs.[306] As a tradeoff for not allowing purchasers of CDs to rip the data from them, record companies are attempting to create purchase incentives by enclosing special features into CD packs, such as plastic cards, which give CD purchasers exclusive access to a special fan-club websites.[307]

File identification technologies adopted by several P2P service providers enable them to identify and track the flow of digital contents in the network.[308] It is possible to tailor these technologies to incorporate a function such as a pop-up box asking for payment whenever the file is downloaded from the central server or a user's hard drive.[309]

Other measures will be necessary when content providers directly supply digital contents to consumers in an effort to protect copyrighted materials from unauthorized reproduction and effectively collect royalties for copyright owners.[310] For example, IBM's Electronic Media Management System ("EMMS") provides features for security, rights management, reporting, and payment interfacing, including features that enable content owners to define usage conditions along the distribution chain. Theoretically, an initial distributee may have full usage rights with recipients having more limited preview rights until full usage rights are purchased, or content owners may be allowed to define content usage conditions by geo-

302. *See Napster Police*, *supra* note 293.

303. *Id.*

304. Charles C. Mann, *First 'Napster-Proof' CD Set to Burn*, CD MEDIA WORLD (Apr. 2, 2001), *at* http://www.cdmediaworld.com/hardware/cdrom/news/0104/napster-proof_cd.shtml.

305. *See id.*

306. *Id.*; *see also* John Borland, *Compromise for CD Copying Is in the Works*, CNET NEWS.COM (Sept. 28, 2001), *at* http://news.cnet.com/news/0-1005-201-7320279-0.html.

307. *Id.*

308. Kahney, *supra* note 141.

309. *Id.* (last visited Oct. 13, 2001).

310. *See generally IBM Software: Database and Data Management: IBM Electronic Media Management System*, *at* http://www-4.ibm.com/software/is/emms/ ("The Electronic Meida Management System (EMMS) from IBM is an e-commerce software solution for digital distribution of media.") (last visited Sept. 7, 2001).

graphic regions.[311] IBM boasts that this technology will allow P2P file sharing and, at the same time, secure a means for compensation to copyright owners.[312]

Under the AHRA, digital recording devices must have Serial Copy Management Systems ("SCMS").[313] Record companies have been struggling to put together the Secure Digital Music Initiative ("SDMI") in the hope that their specifications will be employed by the on-line music distribution business.[314] So far, SDMI has not been able to develop specifications for protecting technology[315] and doubt has been cast as to whether SDMI-led security technology would be the best choice for content providers.[316] Nonetheless, EMMS and WMT (developed by Microsoft) have been adopted by major online music distribution services established in Japan as early as December 1999.[317] These technologies strictly control and limit usage by confining the playing of downloaded music to those digital audio players that comply with SDMI standards.[318] The music downloaded under these technologies can only be transferred to portable players that comport to the digital rights management system and can be transferred from hard

311. Press Release, IBM, IBM to Introduce Superdistribution Capabilities for Advancement of Digital Music Marketplace (Jan. 22, 2001), *available at* http://www-4.ibm.com/software/emms/pdfs/emms_midem_superdistribution.pdf. EMMS is an electronic media distribution and digital rights management system designed to support a broad range of media types, *e.g.*, music and video content. *Id.*

312. Evan Ratliff, *IBM's P2P: Pay-to-Play*, WIRED (Apr. 2001), http://www.wired.com/wired/archive/9.04/mustread.html/mustread.html?pg=2. EMMS has an open architecture to allow technological advances in audio compression, encryption, formatting, watermarking, and end-user devices and applications to be integrated. *IBM Software: Database and Data Management: IBM Electronic Media Management System*, *at* http://www-4.ibm.com/software/is/emms/ (last visited Sept. 7, 2001).

313. 17 U.S.C. § 1002 (Supp. V 1999).

314. Ryan S. Henriquez, Comment, *Facing the Music on the Internet: Identifying Divergent Strategies for Different Segments of the Music Industry in Approaching Digital Distribution*, 7 UCLA ENT. L. REV. 57, 87 (1999). SDMI is a forum of about 200 companies that hope to develop a voluntary, open framework for playing, storing, and distributing digital music in a protected form. *SDMI—Home*, *at* http://www.sdmi.org/ (last visited Sept. 24, 2001). SDMI participants include music content, consumer electronics, information technology, and wireless telecommunication companies. *Id.*

315. Brad King, *Can Napster Secure SDMI?*, WIRED NEWS (Nov. 2, 2000), *at* http://www.wired.com/news/culture/0,1284,39905,00.html. SDMI is currently testing six security technologies, including watermarking, which is designed to destruct music quality when removed from the digital contents. A & M Records, Inc. v. Napster, Inc., 114 F. Supp. 2d 896, 927 n.31 (N.D. Cal. 2000).

316. King, *supra* note 315. SDMI "issued a challenge to crackers, inviting them to attempt to break the encryption [on six files] without destroying the music file." *Id.* An unofficial report revealed that all six were compromised. *Id.*

317. *See, e.g.*, *Du-ub.com*, *at* http://www.du-ub.com/ (last visited Oct. 6, 2001) (on file with author).

318. *See id.*

drive to portable players for a limited number of times (typically, three times).[319] What is more, if the user re-installs or upgrades the operating system, or changes the CPU or hard drive, the music file will not play.[320] These features restrict the use of contents more than the system of physical CD distribution.[321] Thus, it is a market question whether consumers will be able to adjust to this new environment to enjoy music.[322]

It may be more effective to impose upon hard drive and other storage media manufacturers to incorporate protection mechanisms into their products.[323] "Hardware-based protections could prove [to have] a much stronger layer of protection"[324] because they would be less vulnerable to malicious attack. However, wide adoption of such technological protection may take time.[325] A group of hardware manufacturers attempted to create a technology called Content Protection for Recordable Media ("CPRM"), which would have added a piracy-blocking mechanism.[326] This mechanism would stop protected contents from being transferred to a hard drive equipped with CPRM technology.[327] The National Committee on Information Technology Standards ("NCITS") rejected their proposal to incorporate CPRM into the standard rules governing the way computer drives communicate with each other.[328]

Nonetheless, some hardware manufacturers are moving toward this protection technology.[329] Such developments present not only free speech

---

319. *See id.*

320. *See id.*

321. Until recently, consumers have made clear that they wanted non-encrypted MP3s instead of encrypted contents. Evan Hansen, *Digital Songfest Could Fall Flat*, CNET NEWS.COM (Apr. 5, 2001), *at* http://news.cnet.com/news/0-1005-200-5510393.html.

322. *Compare with* Universal Studios, Inc., v. Reimerdes, 111 F. Supp. 2d 294 (S.D.N.Y. 2000) (By effectively addressing the copyrighted works in digital copy protection technology, content providers may control use of their digital contents as demonstrated in this case.).

323. *See* John Borland, *Hardwiring Copyrights*, CNET NEWS.COM (Mar. 23, 2001), *at* http://news.cnet.com/news/0-1005-202-5211420-0.html [hereinafter *Hardwiring Copyrights*].

324. *Id.*

325. *See generally id.*

326. John Borland, *Hardware Safe from Copy Protection—For Now*, ZDNET NEWS.COM (Apr. 2, 2001), *at* http://www.zdnet.com/zdnn/stories/news/0,4586,5080528,00.html. The "4C Entity," consisting of Intel, IBM, Toshiba, and Matsushita Electric, created CPRM technology and proposed its adoption to the National Committee on Information Technology Standards ("NCITS"). *Id.* The 4C Entity had already successfully introduced Content Protection for Prerecorded Media ("CPPM") into the market, which is used for media including audio on DVDs. *Id.*

327. *Id.*

328. *Id.*

329. Press Release, InterTrust, Matsushita Electric (Panasonic) and InterTrust to Collaborate on Secure Music Distribution (Jan. 10, 2001), *at* http://www.intertrust.com/main/pressroom/pressreleases/2001/010110-mei.html. InterTrust Technologies Corporation, a P2P digital rights management company, produces trusted systems technology that can be installed in personal

and privacy concerns, but also raise the question of the extent to which technology and content providers should be allowed to control what consumers do with their copyrighted products after purchase.[330] The question remains whether consumers would allow strict control of the use of copyrighted contents even after purchase. From a copyright perspective, too much restriction on the use of copyrighted works may tip the balance between copyright protection and public access toward greater copyright protection, making dissemination of copyrighted works more difficult.[331] Too much restriction may even interfere with the first sale doctrine,[332] which limits distribution rights.[333] For now, DMCA anti-circumvention provisions seem to have displaced such concerns,[334] strengthening the trend toward technological protections. Now that digital recording devices are required to incorporate technological protection measures,[335] it may not be long before content providers insist on expanding the definition of digital recording devices. Any further development of this trend will be determined by the market.[336] Although all technological protection measures restrict the way consumers use digital contents to some degree, such restrictions should be regarded as a trade-off for enjoying fast and easily accessible digital contents.

2. Technological Enforcement Measures

Content providers must also take preventive measures against unauthorized use of digital contents that have not been patched with protection technologies described above, such as MP3 files put into distribution on the Internet by purchasers of CDs.[337] Napster has announced that it has retained a file identification service, which allows Napster to locate and iden-

---

computers or portable devices. *See id.* In January 2001, InterTrust announced that Matsuhita Electric adopted this technology for its Secure Digital Memory Card devices. *Id.*

330. *Hardwiring Copyrights*, *supra* note 323.

331. *See id.* In recent history, Circuit City's Divx DVD Player, designed to control the use of digital videos, and Sony's Vaio Music Clip, with an early version of SDMI proposals incorporated, were both fast to fail in the market. *Id.*

332. 17 U.S.C. §§ 106, 109 (1994 & Supp. V 1999).

333. *Id.*

334. *Id.* § 1201.

335. *Id.* § 1002(a).

336. *See generally* Brock N. Meeks, *Digital TV Snowed In by 'Napster Factor,'* ZDNET NEWS.COM (Mar. 16, 2001), *at* http://www.zdnet.com/zdnn/stories/news/0,4586, 2697470,00.html. Cable and satellite companies are proposing restrictions on the recording of digital programming. *Id.* In addition to mandating copy protection, the proposal requires cable operators and broadcasters to "down resolution" of specified digital programming so consumers cannot make high-quality copies. *Id.*

337. *See* von Lohmann, *supra* note 153.

tify music files by wavelength and other characteristics.[338] However, Napster's previous effort to comply with the preliminary injunction order was described as "disgraceful" because its filtering system failed to screen many misspelled music files.[339] Napster's filtering is expected to be much more effective in the future by introducing technology that can identify copyrighted music without relying on file names, which can be manipulated by users and plug-in software.[340]

As P2P file sharing activity inevitably discloses the requesting user's Internet protocol ("IP") address, it is technologically possible to track the distribution of contents and find out who is copying the files.[341] An increasing amount of content providers are attracted to this tracking/surveillance service.[342] These services[343] track the designated contents on the Internet to the IP address.[344] Subsequently, the service or content provider notifies the Internet service provider under the DMCA that a user is engaged in an infringing activity, and thus the service provider should disconnect the user's Internet service.[345] The RIAA and Copyright.net use monitoring software to identify individuals by IP address, and then try to persuade ISPs to stop their customers' infringing activities either by shutting them down or blocking access to subscribers' computers that are offering Napster-like file trading facilities.[346] Some ISPs reportedly responded, but others are reluctant to police content that is stored in their subscribers'

338. Press Release, Napster, Inc., Napster and Relatable Enter Into Agreement (Apr. 20, 2001), *at* http://www.napster.com/pressroom/pr/010420.html.

339. *Napster Filtering Efforts Disgraceful*, *supra* note 287.

340. *See generally id.*

341. Janelle Brown, *Salon.com Technology | Who Is Spying on Your Downloads?*, SALON.COM (Mar. 27, 2001), *at* http://www.salon.com/tech/feature/2001/03/27/media_tracker/index.html [hereinafter *Who Is Spying on Your Downloads?*].

342. *Id.*

343. Media Enforcer and Copyright Agent are examples of these services. *Media Enforcer Products*, *at* http://www.mediaenforcer.com/html/products.html (last visited Nov. 2, 2001); *Copyright Agent—Copyright.net Service Provider*, *at* http://www.copyright.net/csphome/copyrightagent/ (last visited Nov. 2, 2001). One product, Songbird, is available free of charge. *Media Enforcer Products*, *at* http://www.mediaenforcer.com/html/products.html (last visited Nov. 2, 2001).

344. *See Who is Spying on Your Downloads?*, *supra* note 341.

345. *Id.*

346. *Napster Police*, *supra* note 293. There is a similar movement against Gnutella users. *See Busted Over Gnutella*, *supra* note 135. The Motion Picture Association of America has also adopted tracking technology like Ranger Online's Intelligent Online Scanning Technology ("IOS") to track down illegally distributed contents and to notify major Internet service providers ("ISPs") and universities that some people on their networks are violating federal law by using Gnutella. *Id.* As the movie industry is contemplating offering movies on-line before the end of 2001, such a movement is expected to accelerate. Tim Swanson & Pamela McClintock, *Napster Chill Thrills Pic Biz*, VARIETY, Feb. 19–25, 2001, at 35.

hard drives.[347]

There is ambiguity as to whether the DMCA "notification and take down" provisions apply to situations where content is on users' hard drives instead of ISP servers.[348] Evidently, Congress did not consider situations where content was not controllable.[349] The RIAA and Copyright.net assert that unless ISPs comply with their requests, the DMCA safe harbor provisions will not be applicable to such ISPs.[350] Considering that ISPs do not have any control over users' hard drives, it would be difficult to hold ISPs contributorily or vicariously liable for any direct infringement by their users.[351] ISPs do offer Internet connections to users and usually reserve the right and ability to terminate the connection service.[352] The problem is, however, that ISPs are typically unaware of what has been transmitted through the Internet connection. The idea of holding ISPs contributorily or vicariously liable simply because ISPs do not terminate the connection service (which might be used for a vast number of legitimate purposes other than transmitting infringing contents) seems extreme in light of the DMCA's safe harbor provision,[353] which protects ISPs from being held liable for transmitting infringing materials.[354]

Because it would be impractical for content providers to sue each and every user, they could sue a group of individuals to scare other users into good behavior. However, in terms of customer relations, this may do more harm than good because such actions may instead anger consumers. Thus, content providers need to carefully consider the balance between copyright enforcement and public relations.

Finally, the above-mentioned technological enforcement measures may be vulnerable to those decentralized P2P networks that encrypt files that have been dedicated to the network. One reason for this is because of the technical difficulty in locating and identifying the digital contents copyrighted by the content provider. In addition, the DMCA may work against tracking services when the services attempt to decrypt the file to identify

347. *See Napster Police*, *supra* note 293.

348. *Id.*

349. *See id.*

350. *See id.*

351. *See id.*

352. *Id.*

353. 17 U.S.C. § 512(a) (1994 & Supp. V 1999); *see also Napster Police*, *supra* note 293.

354. Of course, if an ISP believed that a user is engaged in an infringing activity, the ISP can terminate the connection service if entitled to do so according to their terms of service. Having no "notice and take down" procedure applicable to § 512(a), ISPs should not be obligated to take the risk of offending their users. *See Napster Police*, *supra* note 293.

it.[355] It remains to be seen the extent to which controversial provisions concerning the prohibition of circumventing technological protection measures should be tailored to allow legitimate uses.

VI. CONCLUSION

Digital technology extends the ways to exploit and recoup investments.[356] Also, it allows copyright holders to control the use of their content.[357] In the era of analogue arts, after copyright holders publicize their works, the works are exposed to the risk of being copied by manual copying, photocopying, or photographing. However, digital copyright owners have technological means to limit the copying or transfer of their works even after publication. This fact alone should not justify unauthorized massive reproduction and dissemination. In the era of on-line distribution, content providers must face technological enforcement reinforced by the copyright legal regime.

Napster IV was decided correctly within the ambit of current legislation and perceptions of limits on copyright infringement liability. Further, as this Article has addressed, it is highly likely that centralized P2P networks can be held liable for copyright infringement not only in the United States, but also in Japan. However, such actions would still be subject to a case-by-case analysis. Current legislation and court attitudes do not permit a complete prohibition on P2P technology, including most of the decentralized P2Ps.[358] Furthermore, P2P systems do have the potential for various legitimate uses.[359]

---

355. Again, the chilling effect of a DMCA violation may deter content providers or P2P surveillance services from decrypting such files. *Id.*

356. *See generally* Hansen, *supra* note 321.

357. *The Digital Revolution*, MACLEAN'S, Nov. 6, 2000, at 33, LEXIS, News Group File, Most Recent Two Years.

358. A & M Records, Inc. v. Napster, Inc., 239 F.3d 1004, 1021 (9th Cir. 2001). The court concluded:

> We agree that if a computer system operator learns of specific infringing material available on his system and fails to purge such material from the system, the operator knows of and contributes to direct infringement.... Conversely, absent any specific information which identifies infringing activity, a computer system operator cannot be liable for contributory infringement merely because the structure of the system allows for the exchange of copyrighted material. To enjoin simply because a computer network allows for infringing use would, in our opinion, violate *Sony* and potentially restrict activity unrelated to infringing use.

Id.

359. *See Is There Room on the Net for P2P?*, *supra* note 147.

In addition, P2P systems are gaining popularity,[360] not only among individuals, but also among big players in the IT field.[361] If P2P technology cannot be banned, it seems impossible to ensure that copyrighted materials are not illegally exchanged in the network. Fast dissemination of digital contents and ease of reproduction available to each user via technological advancement have diluted the public's observance of copyright norms. Content providers are less confident of the copyright legal regime's deterring effects on the public.

As recent announcements by major record companies have revealed, all of the big five labels are putting more strength into starting on-line music distribution businesses.[362] These moves can be understood as a response of the music industry to accommodate and compete in the quickly developing market of on-line music distribution, including those facilitated by P2P technology. By adding and offering incentives like exclusive information on artists and bundling recommendation services, these on-line music distribution services may compete with other services such as the free exchange of music files through independent P2P networks.

---

360. *See, e.g.*, Eytan Adar & Bernardo A. Huberman, *Free Riding on Gnutella*, FIRST MONDAY (Oct. 2, 2000), *at* http://firstmonday.org/issues/issue5_10/adar/index.html. There is a concern that the free-riding nature of a majority of the users may lead to failure of an ideal file-sharing network. *See id.*

361. Press Release, Sun Microsystems, Inc., Sun Microsystems to Acquire Infrasearch; Enhances Project Juxtapose Efforts with Innovative P2P Search Technology (Mar. 6, 2001), *at* http://www.sun.com/smi/Press/sunflash/2001-03/sunflash.20010306.1.html. Sun Microsystems has announced it will further its research by establishing P2P fundamentals that are to become the standard of P2P technology by purchasing InfraSearch, Inc., the company established by the Gnutella developers. *Id.* Intel has also established the P2P Working Group and is working towards standardization of P2P technology and simultaneously developing P2P products. Press Release, Intel Corp., Intel Developer Forum Spring 2001: Keynote by Pat Gelsinger (Feb. 28, 2001), *at* http://www.intel.com/pressroom/archive/speeches/pg20010228idf.htm.

362. *See* Hansen, *supra* note 321. On April 2, 2001, RealNetworks formed a pact with AOL-Time Warner, Bertelsmann and EMI group to establish a new music subscription service on-line called "MusicNet." *Id.* MTVi group and RioPort.com has announced that they would offer paid music downloads from all five major music labels on RadioMTV.com and VH1atWork Radio, beginning April 2001. Press Release, RioPort & MTVi Group, MTVi and Rioport Partner to Become Industry's First to Offer Paid Downloads from All Five Major Record Labels (Apr. 4, 2001), *available at* http://www.rioport.com/riocoprpressreleasespring/1,4283,00.htm. On April 9, Label Gate, a Japanese on-line music distribution company, announced that Universal Music has participated in Label Gate Community, which hosts seventeen record companies in Japan. *See* Press Release, Label Gate, Label Gate Zoushi no Goan-nai [Label Gate Capital Increase] (Apr. 9, 2001), *at* http://www.labelgate.com/press/release5.html (on file with author). Universal was one of the last record companies to join Label Gate Community. *Id.* Reportedly, this type of collaboration is precisely the kind of progress that legislators have been looking for, and the Senate Judiciary Committee would be examining copyright issues raised by music and video distribution on-line. *See* John Borland, *Net Music Breakthrough Brewing*, CNET NEWS.COM (Apr. 2, 2001), *at* http://news.cnet.com/news/0-1005-200-5246693.html.

In the meantime, efforts to technologically enforce and eliminate unauthorized use will and should continue consistent with the various accommodating measures mentioned above. If not, content providers will lose the race against vicious pirates utilizing P2P and other newly emerging technologies. An "arms race" against crackers has been a common phenomenon since the emergence of digital technology. Why should copyright owners let them thrive? For the purpose of the copyright regime, copyright owners must arm themselves and fight to secure their rights.[363] In order to address the problems spawned by digital technology, those problems must be resolved by digital technology.[364]

363. *See* Jayne A. Pemberton, Note, *UPDATE: RIAA v. Diamond Multimedia Systems*, 7 RICH. J.L. & TECH. 6, ¶ 29 (Fall 2000), *available at* http://www.richmond.edu/jolt/v7i1/note3.html.

364. *Id.*