The End of the World as We Know It? The State of Decentralized Peer-to-Peer Technologies in the Wake of *Metro-Goldwyn-Mayer Studios v. Grokster*

MICHAEL SUPPAPPOLA[†]

"Money . . . it's a crime. Share it fairly but don't take a slice of my pie."
Pink Floyd

I. INTRODUCTION

The digital technology revolution is upon us, and both copyright holders and Internet libertarians are firmly entrenched on the legal battleground of peer-to-peer file sharing. The recent spread of decentralized peer-to-peer technology has both intrigued and baffled the courts and legal scholars. The potentially disastrous ramifications for copyright holders and consumers have recently carried the issue of file sharing from a small topic for discussion in legal and technological circles to the spotlight of the national media.[1]

The fact that peer-to-peer technology has the potential to revolutionize the Internet in myriad respects has often been lost in the vast amounts of litigation surrounding the online copyright controversy. New digital technology offers artists and copyright holders an unprecedented opportunity to achieve global exposure with extremely low reproduction and distribution costs.[2] The public benefits of peer-to-peer technology are self-evident: the ability to experience music and visual works at a fraction of the time and cost it would entail to travel to a local music store.

Copyright holders, however, argue that the new technology has a rather unfortunate side effect: peer-to-peer users are able to obtain copyrighted works for free. Large-scale copyright owners such as the

---

[†] Michael Suppappola is a candidate for Juris Doctor at the University of Connecticut School of Law, 2005. He received his Bachelor of Arts at the University of Massachusetts in 2002. The author wishes to thank Professor Lewis Kurlantzick who served as an advisor to this project and whose comments and edits were instrumental to the formulation of this piece.

[1] *See, e.g.,* Jennifer Alsever, *Illegal Net Swapping of Music Plunges*, The Denver Post, Jan. 5, 2004, at E1.

[2] Jennifer Norman, Staying Alive: Can the Recording Industry Survive Peer-to-Peer?, 26 Colum. J.L. & Arts 371 (2003).

members of the RIAA argue that peer-to-peer networks facilitating "internet piracy" will sound the death knell for the financial incentive to create artistic works that has long been safeguarded under the federal Copyright Act. Copyright holders have vociferously attacked file-sharing programs such as Napster, Grokster, and Kazaa with legal challenges designed to stem the tide of Internet piracy. When these attacks have failed, the RIAA has directly sued users of file sharing programs who have downloaded copyrighted works for free.[3] As a result, the RIAA has been widely criticized for the unorthodox public relations strategy of suing its own customers.

Conversely, advocates of peer-to-peer file sharing argue that the new technology satisfies the two purposes behind the granting of copyright protection: "1) providing an incentive to "authors" to create, and 2) providing the public with as much creative product as possible."[4] Professor Michael Landau provides an overview of this argument: "In the case of the digital reproduction and distribution of files…the work has already been created, and a certain number of copies have been legitimately purchased, thereby providing the creator with a royalty, albeit lower than he or she would receive in a perfect world."[5] Therefore, the incentive to create the work has been satisfied, and the public is provided with quick and easy access to artistic works.[6] This argument, however, fails to consider that providing an "incentive" to create necessarily entails providing full protection to "authors and money for works that are proper subject matter of copyright."[7]

This comment endeavors to examine the future of peer-to-peer technology in the wake of *Metro-Goldwyn-Mayer Studios, Inc. v. Grokster, Ltd.*,[8] in which a California District Court dismissed a suit by large-scale copyright holders against decentralized peer-to-peer programs. It will focus on the legal arguments that will help shape peer-to-peer technology in the future, and provide possible solutions to the incessant legal and technological battle over the distribution of copyrighted works through peer-to-peer file sharing.

Part II of this comment provides an overview of how decentralized peer-to-peer technologies work. Part III examines the history of the

---

[3] Alsever, *supra* note 1.
[4] Professor Michael Landau, Digital Music Downloads and Copyright Infringement, 758 PLI/Pat 405, 409 (2003).
[5] *Id*.
[6] *Id*.
[7] *Id*.
[8] Metro-Goldwyn-Mayer Studios, Inc. v. Grokster, Ltd., 259 F.Supp.2d 1029 (C.D.Cal 2003).

Copyright Act, past case law and legislative enactments that have laid the legal foundation for the future of online file sharing. Part IV will focus on the controversial *Grokster* decision, and the reaction by large-scale copyright holders. Part V will analyze the effect other recent decisions concerning file sharing will have upon both copyright holders and the future of decentralized peer-to-peer technology. Finally, Part VI will examine possible solutions to the legal controversy surrounding peer-to-peer file sharing, including legislative action, technological changes, and market correction.

II. HOW PEER-TO-PEER WORKS

Digital technology enables audio recordings to be compressed into a digital file that uses little memory, and therefore enables the recording to be downloaded or uploaded over the Internet with relative ease and only minimal effect on sound quality.[9] Once a user has converted a recording from a compact disk into a digital file on a computer's hard drive, a peer-to-peer file sharing service enables that user to share the file with other users on the same network.[10] Although all peer-to-peer technologies vary in minor respects, there are three generally accepted classes: hybrid, pure, and what I will call "next-generation" technologies.[11]

A. The Napster Model: Hybrid Peer-to-Peer Technology

A hybrid peer-to-peer network is not entirely peer-to-peer because users do not send requests for files directly to other users.[12] Napster is the best-known example of a hybrid peer-to-peer system. Napster was a hybrid system because "it does not completely abandon the local center concept of networks."[13] A user first had to access Napster's Internet site and download "MusicShare" software.[14] After registering with Napster, the user would be given a username and password to log-on to the Napster network. To share files with others, a user had to save his MP3 audio files to a "user library" directory on his hard drive.[15] When a user

---

[9] A&M Records, Inc. v. Napster, Inc., 239 F.3d 1004, 1011 (9th Cir. 2001).
[10] *Id*.
[11] David J. Colletti, Jr., Technology Under Siege: Peer-To-Peer Technology is the Victim of the Entertainment Industry's misguided Attack, 71 Geo. Wash. L. Rev. 255, 264 (2003).
[12] *Id*.
[13] *Id*.
[14] Napster, 239 F.3d. at 1011.
[15] *Id*. at 1011-12.

logged in, the MusicShare software would search his user library for properly formatted MP3 files, and upload the file names from the user's hard drive to the Napster service.[16] The file names would then be stored in a "library" of file names available for transfer during the time the user was logged into the Napster system.[17]

Users were then able to search the Napster library for a particular file name. The search form is submitted to the Napster server, which matched the desired song name with similar file names in the Napster library, and then sent the file name back to the requester.[18] Once the requester selected a file to download, Napster's software obtained the Internet Protocol ("IP") address of the file provider and sent this information to the requester's computer.[19] The requester's computer used the IP address to connect with the provider's "browser software and download(ed) the MP3 file from the host user's library."[20]

While the actual file exchange occurs between the users' computers (as in a "pure" file sharing program), Napster is a "hybrid" technology because users must first search for and locate each other through Napster's central database.[21]

B. The Grokster Model: Pure Peer-to-Peer Technology[22]

Grokster, Morpheus, and Kazaa are examples of "pure" peer-to-peer technologies. Unlike in a hybrid model, there is no need for a central server. At the center of "pure" peer-to-peer systems is a piece of technology that, once downloaded, directly connects users to each other.[23]

"Pure" systems are often labeled "decentralized" because there is not one particular nexus that facilitates the connections between users.[24] A new user "needs only to link to one current user to be virtually linked to everyone with whom the current user is linked."[25] After a user has downloaded the correct software, the role of the software provider (such

---

[16] *Id*. at 1012.
[17] *Id*.
[18] *Id*.
[19] *Id*.
[20] *Id*.
[21] Colletti Jr., *supra* note 11.
[22] A more detailed description of the Grokster "FastTrack" software and StreamCast's "Morpheus" software is offered in Part IV of this comment.
[23] Colletti, Jr., *supra* note 11, at 265.
[24] *Id*.
[25] *Id*.

as Grokster or Kazaa) is non-existent because "pure" peer-to-peer networks are self-operating.[26] These networks "continue to run even when the software provider's computers are unavailable."[27]

C. "Next Generation" Peer-to-Peer Technologies

In many respects, "next generation" peer-to-peer technologies are even more decentralized than "pure" file sharing networks. Similar to "pure" systems, next generation networks require no central server because the users interact directly.[28] Next generation networks, however, also provide an increased amount of efficiency and anonymity.

One type of "next generation" network is the Freenet model. Systems such as Freenet hide the source of file information by encoding the files and passing specialized "keys" which can unlock those files to users.[29] Each user's computer is "only aware of its immediate neighbors."[30] Systems such as Freenet are often described as "law-defying" due to the difficulty in discerning the Identification of users who participate in file sharing on these networks.[31]

A second type of "next-generation" file sharing system is the eDonkey model. This type of system differentiates itself from the earlier "pure" networks in two ways. First, when a file is shared on eDonkey, the "technology gives the file "a 'hash' Identifier – essentially an address based on the characteristics of the file itself."[32] Every computer on the network temporarily serves as an index for a certain number of addresses assigned to it.[33] Thus, while a "pure" decentralized searcher would send a query to each node on a network to find which stores a particular file, eDonkey sends a query directly to the computer that is "temporarily responsible for keeping track of the location of files in that category."[34] The result is a notably quicker response time.

Second, systems such as eDonkey can break up each file into little pieces, which can be distributed independently of the entire file itself.[35]

---

[26] *Id*.
[27] *Id*.
[28] *Id*.
[29] *Id*. at 265-66.
[30] *Id*. at 266.
[31] *Id*. at 265.
[32] John Borland, *File Swapping Shifts Up a Gear*, *available at* http://news.com.com/2100-1026-1009742.html (May 27, 2003).
[33] *Id*.
[34] *Id*.
[35] *Id*.

Once a user begins downloading these pieces, he offers them to the network at large.[36] Thus, a user does not have to download a complete file before it is offered to other users on the network, making "distribution of large files much more efficient."[37]

III. THE EVOLUTION OF COPYRIGHT INFRINGEMENT AND SECONDARY LIABILITY FOR NEW TECHNOLOGIES

A. The Purpose of Copyright Protection

Article I, Section 8 of the United States Constitution reads: "The Congress shall have the power … to Promote the Progress of Science and useful Arts, by securing for limited Times to Authors and Inventors the exclusive Right to their respective Writings and Discoveries."[38] Congress used this power to create the Copyright Act, which grants the copyright holder "exclusive rights to use and to authorize the use of his work in five qualified ways," including reproduction and distribution of the "copyrighted work in copies."[39] The purpose of the Act, however, is not to confer an unlimited monopoly on the work to the creator, but rather to "stimulate artistic creativity for the general public good."[40] The Act attempts to balance the encouragement and reward of creative works with "the cause of promoting broad public availability of literature, music, and the other arts."[41]

When one of the artists' exclusive rights have been violated, case law protects the copyright holder through the doctrines of direct, contributory, and vicarious infringement.[42] In order to prevail on a claim for contributory or vicarious copyright infringement, a plaintiff must first prove direct infringement by a third party.[43] To present a prima facie case of direct infringement, a plaintiff must show (1) ownership of the allegedly infringed material and (2) the alleged infringer(s) violated at least one exclusive right granted to copyright holders under the Copyright Act.[44]

---

[36] *Id*.
[37] *Id*.
[38] U.S. CONST. art. I, § 8, cl. 8.
[39] Sony Corporation of America v. Universal City Studios, Inc., 464 U.S. 417, 433, 104 S.Ct. 774, 784 (1984).
[40] *Id*.
[41] *Id*.
[42] Norman, *supra* note 2, at 372.
[43] *Id*.
[44] *Id*.

Once direct infringement is established, a plaintiff can establish contributory infringement where the defendant with knowledge of the infringing activity, induces, causes or materially contributes to the infringing conduct of another.[45] To prevail on a claim of vicarious liability, the plaintiff must show that the defendant (1) has the right and ability to control the infringer's acts and (2) receives a direct financial benefit from the infringement.[46]

B. The "Sony Rule": Sony Corp. of America v. Universal City Studios, Inc.[47]

The Supreme Court's ruling in *Sony* is the leading case on secondary liability. In *Sony*, large-scale copyright holders of television programs sued Sony over the manufacture and sale of Betamax home video tape recorders. The *Sony* Court rejected the argument that a "product's capability of being used in an infringing manner constituted the knowledge" required to impose contributory or vicarious liability.[48] More importantly, the Court held that contributory infringement requires "an ongoing relationship between the direct infringer and the contributory infringer at the time the infringing conduct occurred."[49] The Court reasoned that "[Sony does] not supply Betamax consumers with respondent's works; respondents do. [Sony] supplies a piece of equipment that is generally capable of copying" both copyrighted and uncopyrighted works.[50]

The Court offered the Staple Article of Commerce Doctrine ("Sony rule") in an attempt to strike a balance between "a copyright holder's legitimate demand for effective – not merely symbolic – protection" and the societal interest in promoting and developing new technologies.[51] Under the Sony Rule, the sale of copying equipment does not constitute contributory infringement so long as the device is "capable of substantial noninfringing uses."[52]

Furthermore, in an action for contributory copyright infringement against the seller of copying equipment, "the copyright holder may not prevail unless the relief that he seeks affects only his programs, or unless

---

[45] *Id*.
[46] *Id*.
[47] 464 U.S. 417, 433 (1984).
[48] Colletti, Jr., *supra* note 11, at 261.
[49] Sony Corporation of America v. Universal City Studios, Inc., 464 U.S. at 437.
[50] *Id*. at 436.
[51] *Id*. at 442.
[52] *Id*.

he speaks for virtually all copyright holders with an interest in the outcome."[53] Thus, if a non-insignificant number of copyright holders authorize or do not object to the copying of their works, the product is said to be capable of significant non-infringing uses.[54]

The Court found that the Betamax was capable of at least one significant non-infringing use; recording a program to be viewed at a later time ("time-shifting").[55] The Court found that a "substantial number of copyright holders . . . would not object to having broadcasts time-shifted by private viewers."[56] Moreover, even unauthorized time-shifting does not constitute infringement because it qualifies as a non-commercial fair use of a copyrighted work by the consumer.[57]

C. Digital Copying: Religious Tech. Ctr. v. Netcom On-Line Comms. Servs., Inc.[58]

In *Netcom*, the copyright owner of Church of Scientology founder L. Ron Hubbard's writings sued Netcom, a large Internet service provider ("ISP"). Dennis Erlich, a critic of Hubbard's works, posted several messages that contained passages of Hubbard's copyrighted works on an Internet newsgroup. "According to a prearranged pattern set by the Netcom software, when a message was posted on the [electronic bulletin board], it would automatically be copied onto Netcom's computer, and then to other computers on the Usenet. The messages on Netcom's computer [were] then available to Netcom's customers."[59]

The court first held that Netcom was not liable for direct copyright infringement of Hubbard's works: "the mere fact that Netcom's system incidentally makes temporary copies of plaintiff's works does not mean that Netcom caused the copying."[60] The court compared Netcom to the owner of a photocopying machine who lets the public make copies with it. Although a few members of the public "may directly infringe

---

[53] *Id*. at 446.
[54] *Id*.
[55] *Id*. at 456.
[56] *Id*.
[57] *Id*.
[58] Religious Technology Center v. Netcom On-Line Communications Services, Inc., 907 F. Supp. 1361 (N.D. Cal. 1995).
[59] Alexander Lindey & Michael Landau, 1 Lindey on Entertainment, Publ. & the Arts § 1:15 (3d ed. 2003).
[60] *Netcom*, 907 F. Supp. at 1368-69.

copyrights, courts analyze the owner's liability under the rubric of contributory infringement."[61]

Religious Technology Center argued that Netcom should be liable for contributory infringement because it had received notice that Erlich had posted infringing material but did nothing to remove the posts or prevent future postings.[62] Thus, according to the plaintiffs, Netcom had knowledge of the infringing activity and materially contributed to the infringing conduct by failing to remove the material.[63]

The Netcom court distinguished this case from that of a landlord who acquires knowledge of infringement by a tenant after the signing of a lease.[64] The court noted that "Netcom not only leases space but also serves as an access provider, which includes the storage and transmission of information necessary to facilitate [a user's] postings to [a message board]. Unlike a landlord, Netcom retains some control over the use of its system."[65] Netcom had the ability to suspend user accounts and prevent access by particular users.[66] Thus, the claim for contributory infringement hinged on Netcom's knowledge of the infringement at the time it "provided its services to allow [the user] to infringe plaintiffs' copyrights."[67]

The court held that there were issues of material fact as to whether Netcom knew or should have known that (1) Erlich's posts infringed the plaintiff's copyrights because the plaintiff's failed to comply with a proof of ownership request, and (2) Erlich continued to send infringing posts after Netcom received a notice of infringement from the plaintiffs.[68]

The court dismissed the plaintiff's claim for vicarious infringement on summary judgment, noting that "[t]here is no evidence that infringement by Erlich in any way enhances the value of Netcom's services to subscribers or attracts new [customers]."[69] Netcom received no financial benefit from Erlich or the electronic message board.[70]

D. Congressional Responses to Copying Technology: The Audio

---

[61] *Id*.
[62] *Id*. at 1373.
[63] *Id*.
[64] *Id*. at 1373-74.
[65] *Id.*
[66] *Id*. at 1376.
[67] *Id*. at 1374.
[68] *Id*. at 1375.
[69] *Id*. at 1377.
[70] *Id*.

Home Recording Act and the Digital Millennium Copyright Act

Congress responded to the *Sony* and *Netcom* decisions by passing legislation designed to further define the boundaries between legal copying and infringement.

In response to *Sony*, Congress passed the Audio Home Recording Act ("AHRA") in 1992.[71] The AHRA "essentially codified the settlement" between Sony and copyright holders."[72] The AHRA allowed consumers to record copyrighted material for personal use: "[u]nder the AHRA, no lawsuit may be brought alleging infringement of copyright based on the . . . noncommercial use by a consumer of [a digital audio recording device or medium] for making digital or analog musical recordings."[73] Nevertheless, the AHRA only protects noncommercial reproduction of copyrighted material, not unauthorized distribution. More importantly, the Ninth Circuit has held that "computers (and their hard drives) are not digital audio recording devices" as defined by the AHRA because "their primary purpose is not to make digital audio copied recordings."[74]

Largely in response to cases such as *Netcom*, Congress passed the Digital Millennium Copyright Act ("DMCA") in 1998. Section 512 of the DMCA was passed primarily to limit the liability of ISPs for "acts of copyright infringement by customers who are using the providers' systems or networks."[75] An ISP is defined as an entity involved in the transmission, routing, or provision of "connections for digital online communications, between or among points specified by a user … without modifying the content of the material."[76] The DMCA provided ISPs, system caches, user storage entities, and information location tools (i.e. search engines) a "safe harbor" if they meet five requirements.[77]

To fall within the safe harbor provision, an ISP cannot (1) initiate the infringing transmission; (2) select the information; (3) select the recipients; (4) store the information to make it available to others; or (5) modify the information.[78] System caches, user storage entities, and

---

[71] Colletti, Jr., *supra* note 11, at 260.
[72] *Id*. In return, the AHRA mandates digital copying technologies to pay royalties to copyright holders.
[73] *Id.* (citing 17 U.S.C. 17 § 1008 (2000)).
[74] *Napster*, 239 F.3d. at 1024. (citing Recording Indus. Ass'n of Am. v. Diamond Multimedia Sys. Inc., 180 F.3d 1072 (9th Cir. 1999)).
[75] In re Verizon Internet Serv., Inc., 240 F. Supp. 2d 24, 27 (D.C. Cir. 2003).
[76] 17 U.S.C. § 512(k)(1)(A) (2000).
[77] 17 U.S.C. § 512(k)(1)(B) (2000).
[78] 17 U.S.C. § 512(a)(1)-(5) (2000).

information location tools must meet similar requirements to qualify for limited liability.

Older "hybrid" peer-to-peer technologies such as Napster may fall under the DMCA's definition of a service provider because these systems retain some control over the central server, and therefore may be viewed as facilitating transmission of online communications among points specified by a user.[79] Nevertheless, decentralized peer-to-peer technologies are unlikely to be covered under the DMCA definition of "service provider." Pure peer-to-peer technologies retain no relationship with a user after the software has been downloaded, and thus lack "involvement" with the user's infringing activity. Nevertheless, even if decentralized peer-to-peer technologies qualified as an ISP, system cache, storage entity, or information location tool, they could not meet the five "safe harbor" requirements of the DMCA.

E. The Ninth Circuit Strikes a Blow to Hybrid Peer-to-Peer Technologies: A & M Records, Inc. v. Napster, Inc.

The legality of peer-to-peer technology first became an issue for the courts with the rise of Napster in the late 1990s. The widespread use of Napster by college-age users prompted large-scale copyright holders to respond by seeking an injunction against the operation of the system.[80] A description of how the Napster program works can be found in Part II of this comment. In addition to the file sharing software, Napster provided technical support to its users, as well as a "chat room" where participating artists could provide information about their music and users could meet to communicate with each other.[81] Napster also offered users a "hotlist" function, where a user could "list" another user whom he had obtained music files from in the past. The user could then access an index of all music files in the "hotlisted" user's library when both users were logged on.[82] Like all other files, the "contents of the hotlisted user's MP3 file (were) not stored on the Napster system."[83]

In seeking a preliminary injunction, A&M Records first claimed that Napster users violated copyright holders' exclusive rights to wholesale reproduction and distribution of their works, thus constituting direct

---

[79] This issue is still largely an open question in the courts.
[80] *Napster*, 239 F.3d at 1011.
[81] *Id*.
[82] *Id*. at 1012.
[83] *Id*. at 1012.

infringement.[84] The plaintiffs sufficiently demonstrated ownership of approximately seventy percent of the files downloaded on Napster.[85] The Ninth Circuit upheld the district court's conclusion that Napster users "who upload file names to the search index for others to copy violate plaintiffs' distribution rights" and those who downloaded copyrighted music violate plaintiffs' reproduction rights."[86]

1. Napster's Fair Use Defense

Napster asserted the affirmative defense of fair use in response to the plaintiffs' charge that users directly infringed copyrighted works.[87] Section 107 of the Copyright Act reads "(T)he fair use of a copyrighted work … is not an infringement of copyright."[88] A court must balance four factors to determine if the direct infringer has a valid fair use defense: (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 work as a whole; and (4) the effect of the use upon the potential market or value of the work.[89]

The Ninth Circuit agreed with the district court that Napster users were not fair users. First, the court concluded that the purpose and character of use of the work was non-transformative and commercial.[90] Although Napster argued that changing the form of the recording from an audio compact disk to an audio file was transformative, courts "have been reluctant to find fair use when an original work is merely retransmitted in a different medium."[91] In affirming the district court's holding that the infringing use was commercial, the court held that commercial use was "demonstrated by a showing that repeated and exploitative unauthorized copies of copyrighted works were made to save the expense of purchasing authorized copies."[92] Thus, the first fair use factor was found in favor of the plaintiffs.

Second, "[w]orks that are creative in nature are 'closer to the core of intended copyright protection' than are more fact-based works."[93] The

---

[84] *Id*. at 1014.
[85] *Id*. at 1013.
[86] *Id*. at 1014.
[87] *Id*.
[88] 17 U.S.C. § 107 (2000).
[89] *Napster*, 239 F.3d at 1014.
[90] *Id*. at 1015.
[91] *Id*.
[92] *Id*.
[93] *Id*. at 1016.

Ninth Circuit affirmed the district court's ruling that the creative nature of music cut against a finding of fair use for Napster.

Third, the court held that the infringement constituted wholesale copying because Napster users were downloading the copyrighted works in their entirety.[94] This third factor also cut against Napster.

Finally, the court held that Napster harmed the market in two ways: (1) Napster reduced CD sales "among college students," and (2) it raised "barriers to plaintiffs' entry into the market for the digital downloading of music."[95] The court explained, "lack of harm to an established market cannot deprive the copyright holder of the right to develop alternative markets for the works."[96] Thus, the court rejected Napster's fair use defense on the basis of all four factors.

2. Sampling and Space-Shifting

Napster's next defense claimed that uses of the software for "sampling" and "space-shifting" were specific examples of fair use.[97] First, Napster argued that users "sample" music on Napster in order to decide whether to buy the recording.[98] The Ninth Circuit affirmed the district court's determination that sampling "remains a commercial use even if some users eventually purchase the music."[99] The plaintiffs' collected royalties by offering song samples to Internet sites, and thus were still suffering a commercial loss from users who "sampled" on Napster.[100] Furthermore, even if sampling increased CD sales, Napster still had no right to "deprive the copyright holder of the right to license the material."[101]

Second, Napster offered the *Sony*-like fair use defense of "space-shifting."[102] However, unlike the "time-shifting" of recording programs for later viewing that was central to the *Sony* decision, Napster claimed that users "space-shifted" music from their legally purchased compact disks to their hard drives in order to enjoy the work at a different location and time.[103] The court held that where *Sony* users time-shifted programs

---

[94] *Id*.
[95] *Id*.
[96] *Id*. at 1017.
[97] *Id*. at 1018-19
[98] *Id*. at 1018.
[99] *Id*.
[100] *Id*.
[101] *Id*.
[102] *Id*. at 1019.
[103] *Id*.

almost exclusively for personal use, Napster users simultaneously distributed the copyrighted work to "millions of other individuals."[104] Thus, Napster's claims of sampling and space-shifting were rejected.

3. Contributory and Vicarious Copyright Infringement

The Ninth Circuit then moved to the crux of the case: the plaintiffs' claim that Napster was liable for both contributory and vicarious copyright infringement.

First, the court agreed with Napster that the *Sony* rule prohibited the court from imputing "the requisite level of knowledge to Napster merely because peer-to-peer file sharing technology may be used to infringe plaintiffs' copyrights."[105] The district court erred in placing "undue weight on the proportion of current infringing use as compared to current and future non-infringing use."[106] Thus, the court left open the possibility that Napster could successfully argue the system's current and future substantial non-infringing uses at trial.

Nevertheless, the Ninth Circuit affirmed the district court's ruling because the evidentiary record at "an early point in the proceedings" supported the district court's finding that the plaintiffs would likely prevail on a claim for contributory infringement. The court found that Napster satisfied the "knowledge" element of contributory infringement because it had "*actual* knowledge that *specific* infringing material was available on its system, . . . could block access to the system by suppliers of the infringing material, and . . . it failed to remove the material.[107] In *Sony*, the videotape recorders were a "free-standing" technology; Napster, however, "retained control over its technology and therefore it had knowledge [of the ongoing infringement]."[108]

Napster satisfied the "material contribution" element by providing the "site and facilities" for infringement.[109] Unlike decentralized peer-to-peer technologies, hybrid models such as Napster had the ability to remove copyrighted file names from being uploaded to its central server. More importantly, Napster had the ability to prevent infringing users from accessing the system upon receiving knowledge of the infringing

---

[104] *Id*.
[105] *Id*. 1020-21.
[106] *Id*. at 1021.
[107] *Id*. at 1022.
[108] Colletti, Jr., *supra* note 11, at 263-6.
[109] *Napster*, 239 F.3d at 1022.

activity, and thus materially contributed to the infringement by failing to act.[110]

With respect to vicarious liability, the Ninth Circuit held that Napster received a financial benefit from the infringing activity because the availability of free copyrighted material acted as a "draw" for customers.[111] The court also held that the plaintiffs satisfied the second element of vicarious infringement (right and ability to control users' acts) because Napster had the ability to police its system by locating infringing material listed on its server and the right to terminate users' access to the system.[112] Converse to decentralized peer-to-peer technologies, Napster retained control over its central server.

The plaintiffs, however, had equal access to locating infringing material on the system via the Napster search engine. The court noted that the district court should place "some of the burden on plaintiffs to provide notice to Napster" of particular copyrighted works available through the system when crafting the preliminary injunction.[113] The Ninth Court stayed the preliminary injunction until the district court could modify it in light of the plaintiffs' shared burden.

4. Napster's Legislative Defenses: The AHRA and DMC

Napster argued that home copying of music files is "noncommercial use" that is protected by the AHRA.[114] The court rejected the argument, stating that the AHRA did not provide immunity for computers or hard drives because their "primary purpose is not to make digital audio copied recordings."[115]

The Ninth Circuit, however, refused to accept the district court's conclusion that Napster did not fall under the "safe harbor" protection for ISPs contained in § 512 of the DMCA.[116] Conversely, the court left the issue of whether Napster could obtain shelter under § 512 to be "more fully developed at trial."[117]

5. Outcome

---

[110] *Id*.
[111] *Id*. at 1023.
[112] *Id*. at 1024..
[113] *Id*. at 1027
[114] *Id*. at 1024.
[115] *Id*.
[116] *Id*. at 1025.
[117] *Id*.

On remand, the district court modified the preliminary injunction in accordance with the Ninth Circuit's ruling.[118] The lawsuit was stayed when Napster filed for bankruptcy in June 2002.[119] Roxio, a California-based CD-burning software designer, purchased Napster at a bankruptcy auction for $5 million dollars.[120] Roxio also purchased licensing agreements from Pressplay, a joint venture of Sony and Universal, for $40 million in May of 2003.[121] The "new" version of the program, Napster 2.0, features over 500,000 songs available for download at the price of 99 cents a song and $9.95 per album.[122]

VI. *METRO-GOLDWYN-MAYER STUDIOS, INC. V. GROKSTER, LTD.*

> *"[H]istory has shown that time and market forces often provide equilibrium in balancing interest, whether the new technology be a player piano, a copier, a tape recorder, a video recorder, a personal computer, a karaoke machine, or an MP3 player." - Judge Thomas for the 9th Circuit in Grokster*[123]

Peer-to-peer file sharing technology found its future in jeopardy following the Ninth Circuit decision in *Napster*. Nevertheless, new decentralized peer-to-peer programs began to appear soon after the original Napster was forced to fold. Large-scale copyright holders attempted to put the final nail in the coffin of file sharing by bringing suit against these decentralized networks in *Grokster*.

Metro-Goldwyn-Mayer Studios and 27 other record labels and movie studios brought suit against Grokster, StreamCast ("Morpheus"), and Kazaa for copyright infringement. The plaintiffs sought $150 million in damages and asked the court for preliminary and permanent injunctive relief, arguing that decentralized peer-to-peer technologies had "in

---

[118] A&M Records, Inc. v. Napster, Inc., No. C99-05183 MHP, 2001 WL 227083, at *1 (N.D. Cal. Mar. 5, 2001).
[119] Norman, *supra* note 2, at 383.
[120] John Fortt, *Napster Returns as Online Music Store*, *available at*http://www.siliconvalley.com/mld/siliconvalley/6970031.htm(Oct. 9, 2003).
[121] Amy Kover, *Napster Readies to Enter Crowded, but Legal Market*, *available at* http://www.taipeitimes.com/News/bizfocus/archives/2003/08/17/2003064133%0D (Aug. 17, 2003).
[122] *Available at* http://news.bbc.co.uk/2/hi/entertainment/3223099.stm. The prices quoted in this Comment are as of February 2004.
[123] Metro-Goldwyn-Mayer Studios, Inc. v. Grokster, Ltd., 259 F.Supp.2d 1029 (9th Cir. 2004).

essence, unlocked the door to every video and record store in the country and invited every person to come in and copy as much as they want, in flat violation" of plaintiffs' copyrights.[124] Grokster and Morpheus filed cross-motions for summary judgment with regard to contributory and vicarious copyright infringement, arguing that they "merely provide software to users over whom they have no control," and thus were not secondarily liable for copyright infringement.[125]

Sharman Networks bought the Kazaa system shortly after the case was originally filed and failed to defend the lawsuit.[126] Thus, the district court's ruling only related to the claims against Grokster and Morpheus.

Both Grokster and Morpheus are pure decentralized peer-to-peer technologies. Neither network contains a central nexus that facilitates searches or transactions between users.[127] Conversely, once a user downloads the software of either system, he transacts exclusively with other users logged on to the network. Nevertheless, Grokster's "FastTrack" software and Morpheus' "Gnutella" system differed in several respects.

A. Grokster's FastTrack Technology

Grokster licensed its FastTrack networking technology from Sharman Networks (Kazaa), and therefore does not "own" the system.[128] Thus, Grokster "does not have access to the source code for the application, and cannot alter it in any way."[129]

To understand how the FastTrack network functions, one must first be conversant with an elementary understanding of "nodes" and "supernodes." A node is an "endpoint on the Internet, typically a user's computer," while a supernode is a form of node that has the "heightened function" of collecting information from other nodes.[130] Individual nodes that use FastTrack "automatically self-select" whether they will function as a regular node or a supernode when a user starts the software; a "user's node may be a supernode one day and not on the following day, depending on resource needs and the availability of the network."[131]

---

[124] Appellants' Opening Brief at 9, Metro-Goldwyn-Mayer, Inc. v. Grokster, Ltd., 2003 WL 22794496 (9th Cir. 2003).
[125] *Grokster*, 259 F.Supp.2d at 1031.
[126] *Id.* at 1032.
[127] *Id*. at 1041..
[128] *Id*. at 1039-40.
[129] *Id*. at 1039..
[130] *Id*. at *1040.*
[131] *Id*.

The groups of nodes and supernodes in the FastTrack system resemble a galaxy of sorts, each cluster of nodes revolving around a single supernode. When a user starts FastTrack, the software is preset with a list of "root supernodes" that connect users to the network by "directing them to active supernodes."[132] Grokster has no control over any root or active supernodes; thus, the "technical process of locating and connecting to a supernode … occurs essentially independently of (Grokster)."[133] A user's search queries are relayed among supernodes, "maximizing the breadth of the search pool and minimizing redundancy in search traffic."[134]

Napster effectively utilized one "supernode" owned and operated exclusively by Napster.[135] This supernode uploaded file names from user computers and facilitated all search traffic on the Napster system. In contrast, Grokster users search for and initiate file transfers "without any information being transmitted to or through any computers owned or controlled by Grokster."[136]

B. Morpheus' Gnutella Technology

Originally, StreamCast's Morpheus technology used the same FastTrack software as Grokster. Morpheus, however, is now based on the "open-source Gnutella peer-to-peer technology," a network that features even more decentralization than FastTrack."[137] Companies such as LimeWire, BearShare and Gnucleus also use the Gnutella software.[138]

A user connects to the Gnutella network by "contacting another user who is already connected."[139] The "initial connection is performed automatically after the user's computer contacts one of many publicly available directories of those currently connected to the Gnutella network."[140] Like Grokster, StreamCast does not control any of the directories.[141]

Unlike the galaxy cluster formation of supernodes in the FastTrack system, Gnutella user requests are passed directly from user to user until

---

[132] *Id*.
[133] *Id*.
[134] *Id*.
[135] *Id*.
[136] *Id*.
[137] *Id*. at 1041.
[138] *Id*.
[139] *Id*.
[140] *Id*.
[141] *Id*.

the sought after file is located. The file transfer is then initiated directly between the two users.[142]

C. Copyright Holders' Argument

The plaintiffs' argued that Grokster and Morpheus "reap millions of dollars in revenue from their online trading bazaar by selling advertising they display to their users while they engage in infringement."[143] They claimed, "90% of the works available on the FastTrack network demonstrably were infringing, and over 70% belonged to (the plaintiffs)."[144]

1. Copyright Holders' Argument: Contributory Infringement

Specifically, the plaintiffs claimed that Grokster and Morpheus should be found liable for contributory infringement because they had knowledge of their users' infringement while providing "support, the site or environment, the audience, (or) the means of direct infringement."[145] First, both networks received actual knowledge of the infringing activity. The plaintiffs argued that because "knowledge of the details of infringement, especially knowledge acquired by direct notice, often comes after the specific infringing acts that are the subject of the notice are completed," a defendant need not have knowledge of infringement only at a time when it can stop the activity.[146] This *Netcom* rule should be limited to ISPs that act as a mere conduit for the transfer of files, and not Napster-like technologies that have knowledge of "the massive, constant infringement over their networks."[147]

The plaintiffs also argued that the *Sony* rule was not applicable to the present case. In *Sony*, "the only contact between Sony and the users of the Betamax … occurred at the moment of sale."[148] Here, as in Napster, Grokster and Morpheus set up "dynamic, ever-changing networks through which they continually interact with their users."[149] Unlike *Sony*, where users made personal copies for time-shifting purposes,

---

[142] *Id*.
[143] Appellants' Opening Brief at 7-8, Metro-Goldwyn-Mayer, Inc. v. Grokster, Ltd., 2003 WL 22794496 (9th Cir. 2003).
[144] *Id*. at 10.
[145] *Id*. at 16.
[146] *Id*. at 20.
[147] *Id*. at 21-22.
[148] *Id*. at 23.
[149] *Id*.

decentralized peer-to-peer users were not engaged in fair use because they enabled and facilitated "unlawful distribution of millions of copies."[150] Finally, the plaintiffs claimed that 90% of the files exchanged on FastTrack were infringing, and thus it was not capable of *substantial* non-infringing uses.[151] The *Sony* rule should not be abused by permitting "minimal (and even hypothetical), commercially insignificant non-infringing uses to immunize massive infringing uses that Defendants can – but refuse to – prevent."[152]

Regarding the element of material contribution, the copyright holders claimed the decentralized peer-to-peer networks supplied "the proprietary software, search engine, and means of establishing connections between their users' computers."[153] The plaintiffs evidenced that both services provided technical support and required users to agree to a contract subjecting them to termination for misconduct.[154] Thus, the defendants could stop contributing to the infringing conduct by terminating those who misuse the system.

2. Copyright Holders' Argument: Vicarious Infringement

Furthermore, the plaintiffs argued that Grokster and Morpheus should be held liable for vicarious infringement because they had the ability to control their networks. First, the defendants' terms of service reserved the right to "ban users and/or block infringing content from their systems."[155] Additionally, the defendants could easily upgrade their software to filter or block copyrighted material available over their service.[156] In fact, both networks currently filter or block "pornographic works, viruses, and bogus files."[157] Thus, Grokster and Morpheus could "with relative ease employ emerging 'digital fingerprinting' technology that would block out a substantial percentage of copyrighted songs."[158] The fact that Napster "employed a centralized index while Defendants now use a decentralized one is both legally and factually irrelevant to the ability and obligation to police infringing conduct."[159] In sum, copyright

---

[150] *Id*.
[151] *Id*. at 24.
[152] *Id*.
[153] *Id*. at 25.
[154] *Id*. at 27.
[155] *Id*. at 31.
[156] *Id*.
[157] *Id*. at 32.
[158] *Id*.
[159] *Id*. at 33.

holders urged the courts to not "stand idle while people give away the property of others."[160]

D. Decentralized Peer-to-Peer Defenses

Project Gutenberg is the oldest all-electronic information provider on the Internet. The goal of Project Gutenberg is to "make information, books and other materials available free of charge to the public at large in a general form that the vast majority of computers, programs and people can easily read, use, quote, and search."[161] All of the Project Gutenberg files have been made available using decentralized peer-to-peer technologies such as Morpheus and LimeWire.[162]

Public interest oriented services such as Project Gutenberg and the Internet Archive benefit tremendously from decentralized peer-to-peer technologies. Web based "distribution of material in such volume can become tremendously expensive," specifically because "web-based publishing requires the host to bear the bandwidth costs associated with traffic to and from its site."[163] Grokster and Morpheus would argue that these services are just a few examples of the many substantial, non-infringing uses of decentralized peer-to-peer technology that should be safeguarded by consistent application of the *Sony* rule.

1. Digital Libertarians' Argument: Substantial, Non-Infringing Uses

StreamCast presented evidence that Morpheus has been regularly used to "facilitate and search for public domain materials, government documents, media content for which distribution is authorized, media content as to which the rights owners do not object to distribution, and computer software for which distribution is permitted."[164] Producers of artistic works, especially new artists who do not have a large record label to promote their work, rely on peer-to-peer technology to gain wider global distribution of their work. Even the "plaintiffs themselves use

---

[160] *Id*.
[161] Brief of Amici Curiae American Civil Liberties Union at 5, Metro-Goldwyn-Mayer, Inc. v. Grokster, Ltd., 2003 WL 22753808 (9th Cir. 2003).
[162] *Id*. at 10-11.
[163] *Id*. at 11.
[164] *Id*. Recently, decentralized peer-to-peer users shared files designed to repair damage inflicted by the fast spreading "blaster virus." *Id*. at 9.

defendants' programs as a kind of Neilson rating system" to gauge the popularity of CDs and unsigned bands that are potential hit-makers.[165]

Furthermore, accepting the plaintiffs' "flawed" study citing that 75% of the files shared on the networks are infringing, there remains over 175 million files for which there is no evidence of infringement.[166] Even if 90% of the files available on Grokster or Morpheus were infringing, this would still leave 70 million non-infringing files. The court should focus its attention upon the value of the non-infringing uses, not the percentage of them; to follow the plaintiffs' approach would be to ban VCRs, CD burners, DVD recorders, photocopy machines, and even perhaps email. To take this argument to its extreme, "Microsoft Word could be banned if copyright holders could show that it is being used X percentage of the time to plagiarize."[167]

Proponents of peer-to-peer technologies also cite political organization as another example of a substantial, non-infringing use.[168] As political campaigns move online, the low cost of peer-to-peer networks as an instrument of distribution make it a "superior alternative to other forms of web-based political organizing."[169] Also, through the use of decentralized peer-to-peer networks, citizens of totalitarian regimes such as China will be able to access information from anywhere in the world without fear of censorship.[170]

Although the plaintiffs emphasized that current peer-to-peer networks are predominantly used for infringement, "predictions about the manner in which a new medium of communication will develop are notoriously unreliable." [171] For example, the plaintiffs in *Sony* feared that home recording would spell the end for the movie industry; conversely, they "experienced a financial windfall" from the new home video industry.[172]

2. Digital Libertarians' Argument: No Ability to Control or Material Contribution to Infringement

---

[165] *Id*. at 12.
[166] *Id*. at 13-14. This number is based on a mid-September 2003 search of files on Kazaa which revealed that there were 704 million files available at the time the program was accessed.
[167] *Id*. at 28.
[168] *Id*. at 14.
[169] *Id*.
[170] *Id*. at 14-15.
[171] *Id*. at 16.
[172] *Id*.

In response to the plaintiffs' contention that decentralized peer-to-peer technology could theoretically screen files for copyright infringement and identify infringing users, Grokster and Morpheus responded that neither technology played any role in the identification or transfer of files. When users search for a file, they do so "without any information being transmitted to or through computers" controlled by either company.[173] Furthermore, Grokster does not use registration to control access, and Morpheus does not even control the initial access of users on the Gnutella network.[174] Although defendants' systems include a filtering mechanism for pornographic files and viruses, only the user can "enable the filter and determine what kinds of files will be screened."[175] The current technology does not give any control of filtering to either system, and it is "unclear whether they would even be able to develop" a mechanism that could filter only infringing files while leaving non-infringing files available.[176] Furthermore, the Supreme Court expressly refused to require Sony to modify its Betamax recorder, such as by including a blocking function or eliminating its ability to record programs.[177]

Apart from the *Sony* rule, the defendants argued that both the *Netcom* and *Napster* decisions required actual knowledge *and* the ability to act upon such knowledge by a defendant before they could be found liable for contributory infringement.[178] Neither Grokster nor Morpheus can prevent individuals from downloading the software nor block infringing users from the networks: the "plaintiffs propose a standard that would hold manufacturers of products with perfectly legitimate uses liable unless they build into those products specific tools for monitoring users or unless they build into those products specific tools for monitoring users or preventing infringement."[179]

Finally, the allegation that decentralized peer-to-peer technologies may have specifically structured their technology so as to avoid exercising control over infringing users can be viewed as a decision with positive public interest ramifications. A "requirement of mandatory centralization or control … will result in dramatically increased … and

---

[173] *Id*. at 17.
[174] *Id*. at 18.
[175] *Id*. at 19.
[176] *Id*. at 20.
[177] *See* Sony Corp. of Am. v. Universal City Studios, 464 U.S. 416, 494 (Blackmun, J., dissenting).
[178] Brief of Amici Curiae American Civil Liberties Union at 23, Metro-Goldwyn-Mayer, Inc. v. Grokster, Ltd., 2003 WL 22753808 (9th Cir. 2003).
[179] *Id*. at 24.

overly zealous censorship by companies that are far more interested in avoiding liability than preserving non-infringing speech."[180] Furthermore, the substantial and non-infringing uses that take place on decentralized networks are entitled to full constitutional protection. Courts should not allow the interests of copyright holders to "eviscerate the other crucial protections contained in the First Amendment" by cutting off all non-infringing users on account of the abuses committed by some users.[181] Such a holding would have extremely negative ramifications for the public, whose "well being depends on scientific advances and technological breakthroughs."[182]

In summary, the defendants argued that Grokster and Morpheus created software that is capable of substantial and valuable non-infringing uses, and that neither system has the ability to prevent infringement by users of the software. Thus, the defendants lack the ability to act upon actual knowledge of user infringement that is necessary for contributory liability. Likewise, the defendants lack the ability to control infringing conduct by its users, and thus cannot be found vicariously liable.

E. The District Court's Decision

1. Contributory Infringement

Judge Wilson held that "it is undisputed that there are substantial noninfringing uses for Defendants' software," and cited "distributing movie trailers, free songs or other non-copyrighted works; using the software in countries where it is legal; or sharing the works of Shakespeare."[183] Wilson noted that *Sony* stood for the proposition that "the existence of substantial noninfringing uses turns not only on a product's *current* uses, but also on potential *future* noninfringing uses."[184] While the attorneys defending Napster produced little evidence of current or future non-infringing uses, the Grokster attorneys provided an abundance of evidence relating to legal uses, such as "to facilitate and search for public domain materials, government documents," as well as the authorized or allowed transfer of media files and computer

---

[180] *Id*. at 32-33.
[181] *Id*. at 34.
[182] *Id*. at 36.
[183] *Grokster*, 259 F.Supp.2d at 1035.
[184] *Id*. at1036.

software.[185] Thus, Grokster and Morpheus could not be held liable "merely because the structure of the system allows for the exchange of copyrighted material."[186]

As the Ninth Circuit explained in *Napster*, the defendants could only be found liable for contributory infringement if they "(1) have specific knowledge of infringement at a time at which they contribute to the infringement, and (2) fail to act upon that information."[187] Although the defendants received notice of the infringing conduct, the notice is "irrelevant if they arrive when Defendants do nothing to facilitate, and cannot do anything to stop, the alleged infringement."[188] Judge Wilson used *Netcom* to illustrate the point: "the contributory infringement claim was to be decided not based on Netcom's knowledge at the time it entered into the relevant user agreement, but rather based on any knowledge acquired or possessed while Netcom contributed to the alleged infringement."[189] Therefore, because Netcom "stored and transmitted the allegedly infringing newsgroup posts at issue," the *Netcom* court held that Netcom's failure to "simply cancel (the end user's) infringing message and thereby stop an infringing copy from being distributed worldwide constitutes substantial participation" in the public distribution of infringing material.[190]

Judge Wilson analogized Napster to Netcom, noting that Napster provide the "site and facilities" for infringing conduct to take place by hosting a "central list of the files available on each user's computer, and thus (served) as the axis of the file sharing network's wheel."[191] When Napster shut down, the "Napster file sharing network disappeared with it."[192]

In contrast to Napster and Netcom, neither Grokster nor Morpheus "provides the 'site and facilities' for direct infringement."[193] The defendants' users connect to the network, conduct searches, and upload/download files, "all with no material involvement of Defendants. If either Defendant closed their doors and deactivated all computers

---

[185] *Id*. at 1035. See Part III, Section D for a more detailed analysis of current and future non-infringing uses.
[186] *Id*. at 1036.
[187] *Id*.
[188] *Id*. at 1037.
[189] *Id*.
[190] *Id*. at 1039.
[191] *Id*.
[192] *Id*.
[193] *Id*. at 1041.

within their control, users of their products could continue sharing files with little or no interruption."[194]

The plaintiffs' evidence that Grokster and Morpheus materially contributed to user infringement consisted of "(1) a handful of isolated technical emails from Grokster and (Morpheus) employees" sent to users who had trouble playing copyrighted media files, and "(2) evidence of previously unmoderated discussion forums" in which Grokster users discussed exchanging files and searched for copyrighted material.[195] Judge Wilson held that this evidence did not prove "substantial" participation in infringement; the technical assistance was not only given *after* the alleged infringement took place, but most of the assistance related to the use of other companies' software.[196]

Finally, in response to the plaintiffs' argument that Grokster and Morpheus can communicate with users and initiate upgrades to their software, Judge Wilson concluded that the defendants distribute and support software that can be used for "both lawful and unlawful ends."[197] Whether Grokster and Morpheus can contact their users and provide updates "says nothing" about whether they actually facilitate or enable the transfer of copyrighted files.[198] Grokster and Morpheus were compared to the makers of copy machines and VCRs; although they know that some users will use their products illegally, and they may "provide support services and refinements that indirectly support such use," there remains no evidence that they have made substantial and active contribution to the infringement itself.[199] Like photocopy machine manufacturers, both networks have a right to support their systems so long as they are used for substantial non-infringing uses. Furthermore, the evidence indicated that the defendants had "undertaken efforts to avoid assisting users" who sought to use their software for illegal means.[200]

2. Vicarious Infringement

---

[194] *Id*.
[195] *Id*. at 1042.
[196] *Id*.
[197] *Id*. at 1043.
[198] *Id*. at 1042.
[199] *Id*. at 1043.
[200] *Id*. at 1042.

Next, Judge Wilson determined that neither Grokster nor Morpheus had the "right and ability" to control users' infringing activity, and therefore could not be held liable for vicarious infringement.[201]

To be liable for vicarious infringement, the networks first must have a specific financial interest in the infringing activity. Judge Wilson held that the defendants derive "a financial benefit from the infringing conduct" because the ability to obtain copyrighted works for free is a "draw" for some users of the defendants' networks.[202] Although users of the software do not pay for the product, the defendants derive a substantial "financial benefit from the infringement."[203]

Neither system, however, had the ability to supervise or restrict access to the file sharing networks. While Napster could monitor and control its central library of files being shared, the defendants "provide software that communicates across networks that are entirely outside Defendants control."[204] Grokster had no access to FastTrack's source code because it was licensed from Sharman Networks; Morpheus' Gnutella network was an open-source system, and thus not controlled by any sole owner.

The plaintiffs argued that the decentralized networks could easily employ "digital fingerprinting" technology to filter a certain percentage of copyrighted songs.[205] In fact, the networks already included optional user-controlled filters for pornographic file names. Judge Wilson responded that the defendants' ability to implement new filtering software was "immaterial," because "the obligation to police arises only where a defendant has the 'right and ability' to supervise the *infringing conduct*."[206] Although the parties disputed whether the networks *could* modify their technology, the current software still does not allow the defendants any control over users: "[t]he doctrine of vicarious infringement does not contemplate liability based upon the fact that a product could be made such that it is less susceptible to unlawful use, where no control over the *user* of the product exists."[207]

Judge Wilson concluded that he was "not blind to the possibility that Defendants may have intentionally structured their businesses to avoid secondary liability," but refused to "expand existing copyright law

---

[201] *Id*. at 1045.
[202] *Id*. at 1043.
[203] *Id*. at 1044.
[204] *Id*. at 1045.
[205] *Id*.
[206] *Id*.
[207] *Id*. at 1045-46.

beyond its well-drawn boundaries."[208] The court advised the legislature to decide whether "steps should be taken to reduce the susceptibility" of decentralized peer-to-peer technologies to infringing uses.[209]

Although maligned by large-scale copyright holders, Judge Wilson's conclusion in *Grokster* was correct. *Grokster* was not merely a case about Internet piracy, but a case about whether companies should be held liable for every wrongful use of the new technologies they create. If technological companies were to be held liable for the infringing conduct of users whom the company had no control over, then the legality of technologies such as VCRs and photocopiers would become suspect. Judge Wilson refused to extend copyright law beyond its "well-drawn boundaries," and thus protected new online technologies from the possibility of a devastating chilling effect.

F. Reaction to the Grokster *Decision*

The reaction of large-scale copyright holders to the *Grokster* decision was one of shock and surprise. Hillary Rosen, the RIAA's president and CEO, released a statement shortly after the ruling: "[b]usinesses that intentionally facilitate massive piracy should not be able to evade responsibility for their actions. We disagree with the District Court's decision that these services are not liable for the massive illegal piracy that their systems encourage and we will immediately appeal."[210]

Conversely, advocates of decentralized peer-to-peer technology were ebullient following the decision. The Electronic Frontier Foundation called the ruling "a striking victory," adding that the case was "about technology, not piracy, and today the court agreed, making it clear that technology companies are not responsible for every misuse of the tools they make."[211]

Professor Michael Landau predicts that so long as the Supreme Court's *Sony* rule survives, software that can be used for both legal and illegal purposes will be found not to infringe: "After Grokster, one can only assume that other file-searching and file sharing programs will proliferate like crazy."[212] The *Sony* rule prevents possible lawsuits against myriad technologies that are capable of infringing uses: "It would be utterly ridiculous to shut down the telephone companies, cable

---

[208] *Id*. at 1046.
[209] *Id*.
[210] Andrews Software Law Bulletin, 16 No. 7 ANSLB 3, at 2 (June 2003).
[211] *Id*. at 1.
[212] Landau, *supra* note 4, at 434.

companies, and satellite companies because some people use the lines and satellites for infringing purposes."[213]

Nevertheless, the *Grokster* decision has already had negative effects on some users of the decentralized software. In September of 2003, the RIAA implemented a strategy of suing users of peer-to-peer technologies for direct copyright infringement.[214] Although criticized by many as a public relations disaster, the RIAA hopes the individual lawsuits will act as a deterrent to file sharing by the public. The short-term results for the RIAA seemed positive; traffic to file sharing sites such as Kazaa, WinMX, BearShare and Grokster dropped by as much as 59 percent from January 2003 to January 2004.[215] The research firm NPD Group claimed that more than a million Americans deleted music content from their hard drives in August, shortly before the lawsuits commenced.[216] Furthermore, a survey by the Pew Internet & American Life Project revealed that only 14 percent of Internet users in December of 2003 downloaded files, down from 29 percent in March of 2003.[217]

Other researchers, however, determined that much of the drop-off in file sharing on specific networks was due primarily to the growth in popularity of lesser-known sites, such as eDonkey and Diet K. Eric Garland, CEO of the Internet-research firm Big Champagne, argued that file sharing "(is) more popular than ever. There has been no net decline in the number of people doing it or the number of files being traded."[218]

In fact, the NPD Group revealed that the number of households downloading rose 6 percent in October 2003 and 7 percent in November 2003 following a six-month decline.[219] A separate survey showed that file sharing climbed from 11 million users in September 2003 to 12 million in October 2003.[220] Some speculated that the rise in downloading was due primarily to the holiday season, or perhaps less media coverage of the RIAA's campaign.[221] Nevertheless, an RIAA

---

[213] *Id*. at 432.
[214] Jennifer Alsever, *Illegal Net Swapping of Music Plunges*, The Denver Post, Jan. 5, 2004.
[215] *Id*.
[216] Damien Cave, *How to Get it Online*, ROLLING STONE, Feb. 5, 2004, at 16.
[217] Jennifer Alsever, *Illegal Net Swapping of Music Plunges*, The Denver Post, Jan. 5, 2004. The RIAA's strategy of filing suit against individual direct infringers is analyzed further in Part V.
[218] Cave, *supra* note 216, at 16.
[219] Alex Veiga, *Report: Illegal Music Downloading Began Climbing in October, Reversing Trend*, Jan. 16, 2004, *available at* http://www.detnews.com/2004/technology/0401/19/technology-37432.htm.
[220] *Id*.
[221] *Id*.

spokesman believed that the lawsuits were having an impact: "[a]ll indicators point in the right direction as sales of CDs, legal downloads and awareness that file sharing copyrighted music is illegal have all increased."[222]

Another possible negative outcome of *Grokster* is a potentially devastating technological arms race between copyright holders and downloaders. Copyright holders may "attempt to make files 'uncrackable' and will probably do anything short of disabling the computer of the party that attempts to access content without authorization."[223] Users "who wish to upload and download will be more creative with respect to decryption."[224]

The RIAA appealed Judge Wilson's decision in *Grokster*. On August 19, 2004, the Ninth Circuit upheld the district court's decision.[225] Judge Sidney R. Thomas, writing for the court, noted that it would be dangerous to re-examine the law in the manner contemplated by Copyright Holders: "(n)ot only would such a renovation conflict with binding precedent, it would be unwise . . . it would also alter general copyright law in profound ways with unknown ultimate consequences outside the present context."[226] The Ninth Circuit cautioned courts to exercise caution when reforming traditional legal doctrines to fix problems created by new technologies:

> [W]e live in a quicksilver technological environment with courts ill-suited to fix the flow of internet innovation. The introduction of new technology is always disruptive to old markets . . . (y)et, history has shown that time and market forces often provide equilibrium in balancing interests, whether the new technology be a player piano, a copier, a tape recorder, a video recorder, a personal computer, a karaoke machine, or an MP3 player. Thus, it is prudent for courts to exercise caution before restructuring liability theories for the purpose of addressing specific market abuses, despite their present magnitude.[227]

---

[222] *Id*.
[223] Landau, *supra* note 4, at 435.
[224] *Id*.
[225] Metro-Goldwyn-Mayer Studios, Inc. v. Grokster Ltd., 2004 WL 1853717 (9th Cir. 2004).
[226] *Id*. at *9.
[227] *Id*.

V. *AIMSTER* AND *VERIZON*: FURTHER SHAPING THE FUTURE OF PEER-TO-PEER TECHNOLOGY

Shortly following the California district court decision in *Grokster*, two additional cases were decided that further defined the future of decentralized peer-to-peer technologies. In *In re Aimster*, the Seventh Circuit upheld a preliminary injunction against the Aimster system, a file sharing service that allowed users to find users with whom they could exchange copyrighted works.[228] In *Recording Industry Association of America, Inc. v. Verizon Internet Services, Inc.*, the District of Columbia Court of Appeals held that the DMCA does not authorize copyright holders to discern the Identities of peer-to-peer users through the issuance of subpoenas to ISPs that act as conduits for file sharing.[229]

A. In re Aimster*: Another Defeat for Hybrid Peer-to-Peer Systems*

Aimster was an Internet file sharing service available exclusively to registrants of AOL's instant–messaging service. While a user was exchanging instant messages with a "buddy," the Aimster system allowed the user to attach files to his communication that he desired to share with his buddy.[230] The sender could encrypt all communications between the buddies "by means of encryption software furnished by Aimster as part of the software package" that could be downloaded from Aimster's Web site at no charge.[231] An Aimster user could designate any and all users of the Aimster system as his buddies.

Users could create a user library that listed all the files they were willing to share. A user who wanted to make a copy of a file logged into the system and searched for the desired file name. Aimster's server then searched "the computers of those users of its software who are online," and if it found the file that had been requested, it would "instruct the computer in which (the file) is housed to transmit the file to the recipient via the Internet for him to download on his computer."[232] Thus, the file could enter the recipients' library and become available to all other Aimster users.

---

[228] In re Aimster Copyright Litigation, 334 F.3d 643 (7th Cir.2003).
[229] Recording Industry Association of America, Inc. v. Verizon Internet Services, Inc., 351 F.3d 1229 (C.A.D.C. 2003).
[230] *Aimster*, 334 F.3d at 646.
[231] *Id*.
[232] *Id*.

Large-scale copyright holders sued Aimster for contributory and vicarious copyright infringement. The district court entered a broad preliminary injunction against operation of the system, which Aimster appealed to the Seventh Circuit.[233]

1. Contributory Infringement

Judge Posner rejected both the plaintiffs' narrow reading of the *Sony* rule and the defendants' broad interpretation: "To the recording industry, a single known infringing use brands the facilitator as a contributory infringer. To the Aimsters of this world, a single non-infringing use provides complete immunity from liability. Neither is correct."[234]

Aimster's system possessed two features that shifted this balance toward secondary copyright infringement. First, the Aimster "tutorial" gave as its "*only* examples of file sharing the sharing of copyrighted music . . . ."[235] Judge Posner found the tutorial to be "the invitation to infringement that the Supreme Court found missing in *Sony*."[236] Second, the defendants offered a "Club Aimster" feature that allowed users to download the music most often shared by Aimster users for a monthly fee of $4.95. Club Aimster listed only the 40 most popular songs, all of which were "invariably" under copyright.[237] This served as evidence that Aimster, like Napster, made use of something akin to a centralized server.

Moreover, Aimster failed to "produce any evidence that its service has ever been used for a non-infringing use, let alone evidence concerning the frequency of such uses."[238] Thus, the Seventh Circuit concluded that Aimster demonstrated no substantial, non-infringing uses for the system.

In addition, Judge Posner noted that even when there are substantial non infringing uses of a system, the "provider of the service must show that it would have been disproportionately costly for him to eliminate or at least reduce substantially the infringing uses."[239] Aimster failed to present evidence that the encryption software that was "effective against (Aimster) itself" added any value to the service or reduced cost.[240] The

---

[233] *Id*.
[234] *Id*. at 651.
[235] *Id*.
[236] *Id*.
[237] *Id*. at 652.
[238] *Id*. at 653.
[239] *Id*.
[240] *Id*.

only reason Aimster provided encryption software was to "blind itself in the hope that by doing so it might come within" the *Sony* rule.[241] In sum, the court held that Aimster was likely to be found a contributory infringer because the system had no substantial non-infringing uses, and Aimster had knowledge of users' infringing activity at a time when Aimster could have simply eliminated the encryption feature and thus monitored the use of its system.

2. Vicarious Liability and the DMCA

Judge Posner was uncertain as to whether Aimster could also be held liable for vicarious infringement. Nevertheless, he considered the question of whether Aimster was vicariously liable as merely "academic" since the preliminary injunction could be upheld on the contributory infringement claim.[242] Posner's dicta, however, questioned whether the Supreme Court could have held Sony vicariously liable for failure to "reduce the likelihood of infringement" through a design change.[243] Similarly, Aimster could have easily gained the right and ability to control the system by eliminating its encryption feature and monitoring use. Nevertheless, Judge Posner merely posed the question as to whether failure to effectuate a simple design change could make a system a vicarious infringer. No answer was forthcoming.

In its defense, Aimster claimed that it qualified as an "ISP" and thus fell under the safe harbor provision of the DMCA.[244] Although Aimster qualified as a provider of online services or network access, the court refused to grant safe harbor because the DMCA required ISPs to discourage repeat infringement.[245] By teaching its users how to encrypt illegal file transfers of copyrighted material, Aimster failed to take the required steps under the DMCA safe harbor provision, and thus did not qualify.[246]

Although the *Aimster* decision landed a further blow to hybrid peer-to-peer networks, the Seventh Circuit's decision did not affect the *Grokster* holding or pure decentralized peer-to-peer networks in general. Like Napster, Aimster owned and had complete access to its network. Aimster could terminate users and, with the exception of users who took

---

[241] *Id*.
[242] *Id*. at 654-55.
[243] *Id*. at 654.
[244] *Id*.
[245] *Id*.
[246] *Id*.

advantage of the encryption software, monitor use of the system. As discussed above, decentralized peer-to-peer networks have no such ability to prevent illegal use of the software once users have downloaded it. Furthermore, the defendants in *Grokster* provided ample evidence of substantial, non-infringing uses of their networks; Aimster failed in this respect.

B. RIAA v. Verizon*: A Minor Victory for Decentralized Peer-to-Peer Users*

In response to the *Grokster* decision, the RIAA threatened to sue users of decentralized peer-to-peer networks for illegally downloading copyrighted works. However, the RIAA was heavily dependent upon ISPs to discern the identities of infringers. The RIAA could identify the screen name of a user, and trace the user to his ISP using the Internet Protocol (IP) address associated with that screen name, but only the ISP could identify the name and address of the user belonging to the IP address.[247] Therefore, the RIAA relied on § 512(h) of the DMCA to compel ISPs to disclose the names of alleged infringers.[248] On July 24, 2002 the RIAA served Verizon with a § 512(h) subpoena.[249] Verizon refused to disclose the name of the subscriber, arguing that § 512(h) was inapplicable to ISPs who merely acted as conduit for information transferred between users.[250]

1. A Statutory Trip Through § 512 of the DMCA

Section 512(h) contains a "subpoena provision" that compels ISPs to disclose the names of subscribers whom the RIAA has reason to believe are infringing copyrights.[251] Verizon argued that subsection (h) does not extend to subsection (a) service providers (passive conduits), but only to subsection (c) providers that store the infringing material.[252] The "fact that subsection (h) requires copyright owners to submit, among other documents, 'a copy of a notification described in subsection (c)(3)(A)' provided a basis for Verizon's interpretation of the statute."[253] This

---

[247] *Verizon*, 351 F.3d at 1232.
[248] *Id*.
[249] *Id*.
[250] *Id*. at 1233.
[251] *Id*. at 1232.
[252] Norman, *supra* note 2, at 393.
[253] *Id*.

"notification requirement" is not referenced in subsection (a), which covers passive conduits. Thus, Verizon argued that subsection (h) only applied to subsection (c) providers that store information.[254] Conversely, the RIAA argued that § 512(h) applied to "all situations where an individual uses (the) service provider's networks" to infringe a copyright.[255]

The district court followed the RIAA's interpretation of § 512(h), and ordered Verizon to comply with the RIAA's subpoenas. Verizon appealed to the District of Columbia Circuit Court of Appeals.

2. The Appeals Court Holding

The court began its analysis with the language of § 512(h) itself. Section 512(h)(2)(A) mandates that a proposed subpoena contain "a copy of a notification" of infringement described in § 512(c)(3)(A), which mandates that the subpoena identify the material "to be removed or access to which is to be disabled" by the ISP.[256] Section 512(h)(4) makes the Identification provision of § 512(c)(3)(A) a condition precedent to the issuance of a subpoena.[257] The court noted that Verizon cannot "remove or disable one user's access to infringing material resident on another user's computer because Verizon does not control the content on its subscribers' computers."[258] Therefore, the RIAA's notification "[i]dentifies absolutely no material Verizon could remove or access to which it could disable," and thus § 512(c)(3)(A) "concerns means of infringement other than (peer-to-peer) file sharing.[259]

Second, the fact that § 512(h) contains three separate references to § 512(c) and none to § 512(a) "suggests the subpoena power … applies only to ISPs engaged in storing copyrighted material and not to those engaged solely in transmitting it on behalf of others."[260] Furthermore, the legislative history of the DMCA reveals that the Act never contemplated file sharing: "the legislative history of the DMCA betrays no awareness whatsoever that internet users might be able to exchange files containing copyrighted works."[261] In sum, the court held that § 512(h) did not apply to ISPs acting as passive conduits, and therefore

---

[254] *Id*.
[255] *Id*.
[256] *Verizon*, 351 F.3d at 1234-35.
[257] *Id*. at 1235.
[258] *Id*.
[259] *Id*. at 1236.
[260] *Id*. at 1236-37.
[261] *Id*. at 1238.

Verizon and other passive ISPs did not have to comply with the RIAA's subpoena requests.

3. The Implications of Verizon *for Copyright Holders*

The *Verizon* decision presented a serious roadblock to the RIAA's strategy of directly suing users of decentralized peer-to-peer networks. The RIAA now must file a "John Doe" lawsuit against the infringer, followed by a Federal Rules of Civil Procedure Rule 45 third-party subpoena against the ISP.[262] The ISP would then have to inform the "John Doe" infringer of the federal complaint. This method places "an enormous additional burden on copyright owners, as well as on the federal courts."[263] The process of filing individual "John Doe" suits is not only lengthy and costly, but is also damaging to the RIAA's strategy for filing suits. Under § 512(h), the RIAA could collect millions of names by filing a single subpoena; it could then pick out "the most favorable for a lawsuit against the user community."[264] However, the RIAA must now file individual lawsuits against unknown users. The result could be a public relations disaster. The RIAA had already come under heavy criticism for filing suit against a 66-year-old retired teacher who had never heard of most of the copyrighted songs she was accused of downloading, a 12- year-old girl, and a Hunter College senior who decimated her savings to pay off a $2,500 settlement.[265]

Nevertheless, the RIAA responded to the *Verizon* decision by filing 532 "John Doe" suits on January 21, 2004. RIAA president Cary Sherman said, "[o]ur campaign against illegal file sharers is not missing a beat. The message to illegal file sharers should be as clear as ever."[266]

V. SOLUTIONS TO THE CONFLICT OVER DECENTRALIZED PEER-TO-PEER TECHNOLOGIES

"War...what is it good for? Absolutely Nothing." – Edwin Starr

---

[262] Norman, *supra* note 2, at 394.
[263] *Id*. at 394-95.
[264] *Id*. at 395.
[265] *See* David Kushner, *The RIAA Comes for Your Children . . . and Grandparents*, ROLLING STONE, Sept. 2003, *available at* http://www.rollingstone.com/news/story/_/id/5935911.
[266] Ted Bridis, *Record Industry Files 532 'John Doe' Suits Against Music Downloaders*, Jan. 21, 2004, *available at* http://sfgate.com/cgibin/article.cgi?file=news/a/2001/1/21/national1225EST0557.DTL.

Digital libertarians and proponents of decentralized peer-to-peer networks may have won the first battle with the *Grokster* decision, but the war is far from over. Large-scale copyright holders have vowed to continue bringing suit against decentralized technologies and their users. Outside the courts, a technological arms race has been brewing between copyright owners and file sharing technology. Networks such as Kazaa have been a hotbed for the spread of viruses and corrupted files. However, the copyright holders' digitized guerilla tactics have been unable to keep up with the constant influx of new file sharing sites.

The fight over peer-to-peer technology has been accentuated by both parties' refusal to see the issue of copyright infringement from a neutral standpoint. Peer-to-peer networks, and more specifically their users, refuse to acknowledge that intangible music files are just as much "property" as a compact disk or record. They see the benefits of easy access to artistic works for the general public, but refuse to recognize the financial harm caused to copyright holders, music publishers, and artists. They enjoy the free exchange of works, but deny that copyright holders should be compensated for the original investment and expenditure of resources that helped bring about the work in the first place.

Similarly, in their zealousness to protect their works, copyright holders refuse to acknowledge that new digital technologies have opened up new markets that, if utilized, hold a potential financial windfall for music distributors in the future. More surprisingly, large-scale copyright holders have refused to recognize that the "strategy" of suing their own consumers is not only ineffective, but a terrible business decision. Many users of peer-to-peer networks also buy the "tangible" forms of the downloaded music; thus, the RIAA is bringing suit against the very consumers that they profit from. The RIAA's "campaign" against peer-to-peer users has resulted in the biggest public relations disaster in recent memory.

Thus far, few possible solutions to the conflict have been proffered by either side. Nevertheless, both the recording industry and peer-to-peer networks are in dire need of a solution that will satisfy both parties while keeping intact the delicate balance between artists' incentive to create and the public's right to enjoy and benefit from copyrighted works.

A. Proposed Legislative Solutions: 107th and 108th Congress

1. Author, Consumer, and Computer Owner Protection and Security Act of 2003

On June 19, 2003, Michigan Representative John Conyers and California Representative Howard Berman introduced H.R. 2752, a bill entitled the "Author, Consumer, and Computer Owner Protection and Security Act of 2003."[267] Congressman Conyers said, "[d]igital piracy is one of the biggest problems facing creators of copyrighted content … [t]hat is why Congressman Berman, myself, and other Judiciary Committee members are introducing legislation to give consumers, law enforcement, and content creators the tools they need to protect their rights."[268]

Title III of the Act provides that the "placing of a copyrighted work, without the authorization of the copyright owner, on a computer network accessible to members of the public who are able to copy the work through such access shall be considered to be the distribution, during a 180-day period, of at least 10 copies of that work with a retail value of more than $2,500."[269] In other words, the bill would consider it a crime to make any copyrighted material available under any circumstances without the prior authorization of the copyright owner. The bill also makes it a criminal offense for a software provider to fail to warn a prospective peer-to-peer software user of the "security and privacy" risks presumed by the legislation to be inherent in use of such software.[270]

The Conyers Bill would thus make it a crime to upload or download any copyrighted material on a peer-to-peer network without first obtaining the copyright holder's consent. The most glaring problem with this provision is its disregard of the doctrine of fair use. The bill "would radically narrow existing consumer rights under copyright law and cripple the use of peer-to-peer technology for non-infringing purposes, including research, criticism and news reporting."[271] In sum, the Conyers Bill tips the scale of protection too far in favor of copyright holders, at the expense of the very consumers it claims to protect.

2. Piracy Deterrence and Education Act of 2003

---

[267] H.R. 2752, 108th Cong. (2003).

[268] Press Release, Representative John Conyers, Conyers and Berman Introduce Legislation to Protect Against Online Threats (July 16, 2003), *available at* http://www.house.gov/judiciary_democrats/hr2752intropr71603.pdf.

[269] H.R. 2752, 108th Cong. (2003).

[270] *Id*.

[271] P2P United.org, *H.R. 2752, "Author, Consumer and Computer Owner Protection and Security Act of 2002, available at* http://www.p2punited.org/modules.php?op=modload&name=News&file=article&sid=16&mode=thread&order=0&thold=0.

Texas Representative Lamar Smith sponsored H.R. 2517, the Piracy Deterrence and Education Act of 2003. If passed, this bill would direct the FBI to develop a program to deter the public from illegally downloading copyrighted material.[272] Copyright owners would also be allowed to use the FBI seal to deter illegal transfers of copyrighted files.[273]

Peer-to-peer advocates attacked the provision of the bill allowing use of the FBI seal, claiming "the average viewer of such a notice will be likely to assume incorrectly that lawful conduct under present copyright law could subject him or her to prosecution or penalty."[274] This minor quibble aside, this bill's major flaw is that it is largely irrelevant. If consumers are not deterred by the RIAA's lawsuits, it is difficult to envision that an FBI educational program or use of the FBI seal would significantly deter illegal file sharing.

3. Past Legislative Proposals: The Berman Bill

Other attempts to curb illegal downloading of copyrighted files were defeated in the 107th Congress. The most notable of these was a bill introduced by Representative Berman that essentially would allow a copyright owner to disable, interfere with, block, divert, or "otherwise impair" the unauthorized distribution of his work on a peer-to-peer network, so long as he did not "alter, delete, or otherwise impair the integrity" of the user's computer.[275] The copyright owner would have to first notify the Department of Justice of the means of impairment, and is prohibited from causing damage in excess of $50.00 to the user's computer.[276]

Like the Conyers Bill, the Berman Bill weighed far too heavily in favor of copyright holders. First, the bill required a loss in excess of $250.00 before a user could sue for wrongful impairment.[277] Second, an individual would have to show that the copyright owner had "no

---

[272] *Id*.
[273] H.R. 2517, 108th Cong. (2003).
[274] P2P United.org, *H.R. 2517, "Piracy Deterrence and Education Act of 2003," available at* http://www.p2punited.org/modules.php?op=modload&name=News&file=article&sid=17&mode=thread&order=0&thold=0
[275] H.R. 5211, 107th Cong. (2002).
[276] Norman, *supra* note 2, at 399.
[277] *Id*.

reasonable basis" to believe that his copyright was infringed.[278] This would be extremely difficult for a user to prove; moreover, a copyright owner could use technological self-help against a fair user so long as he had a "reasonable basis" for believing the use was infringing.[279] The bill eventually failed, primarily because it was ostensibly hostile to the rights of consumers.

To truly be effective, future legislative proposals must strike a fair balance between the rights of copyright holders and peer-to-peer consumers. Some commentators have put forth the idea of a bill that makes it illegal for peer-to-peer networks to profit from unauthorized copyright distribution.[280] This would have little effect, however, on "word-of-mouth" networks such as Gnutella that do not depend on advertising or profit to attract users. Furthermore, it has become obvious that online "anarchists" will continue to develop peer-to-peer networks for the sheer joy of creating them. In contrast to real world services, those in the online world are unlikely to be controlled by withholding economic incentive.

Congress will be hard pressed to find a solution that benefits copyright holders without outlawing important aspects of current peer-to-peer technology. Instead of passing bills that sponsor "educational" campaigns concerning the illegality of peer-to-peer file sharing, the better choice may be for Congress to refrain from legislative intervention altogether. Legal "pay-per-use" sites such as iTunes and Musicmatch offer faster downloads, easier interfaces, and a greater selection of songs. Thus, these pay-per-use sites may deflect consumers from "free" peer-to-peer technologies simply by offering a better alternative in the market. *If* an effective legislative solution is to be found, however, it will inevitably have to put the weight of the law behind a new technology that curtails illegal copying.

B. Technology Solutions

Perhaps a more viable solution is to fight technology with technology. Copyright violators on peer-to-peer networks rely on several technological devices to illegally copy works. First, a user must make use of a CD burner to compress a piece of music into an audio file. Second, the user must register with a peer-to-peer network in order to upload the file so other users may download the file for free. The

---

[278] *Id*.
[279] *Id*. at 400.
[280] *Id*. 400-01.

solution to the peer-to-peer conflict may lie in the control of these technologies.

1. Digital Rights Management Systems

Perhaps the answer to the online copyright dilemma is to build digital "fences" around the material. Digital fences are often used to prevent unauthorized access of online entities. One cannot access an email account without a username and password; most pornographic web sites are restricted to those who can verify they are 18 years old; files that are "streamed" to users are copy-protected, and thus disappear once the stream is completed. Can copyright holders protect their works through similar means?

Some legal scholars have argued that technological restrictions on compact disks will help stem the tide of illegal copying. Professor Landau proposes a scenario where each CD sold has a "registration number" and "password" that allows a purchaser unlimited access to the CD for copying purposes.[281] The authorized user would be able to make unlimited fair use of the CD; however, a "friend" who attempts to copy the CD would be unsuccessful unless they also purchased the CD.[282] If the "friend" attempts to crack the anti-circumvention technology, they would be in violation of § 1201 of the DMCA.

Professor Landau's hypothetical is clearly fraught with problems. The copy protection on the CD would not prevent the user from personally uploading the files to a peer-to-peer site. Furthermore, most users would simply pass on the authorization codes to their friends. However, the *theory* of copy protection devices that may effectively stop a CD from being transferred off one's hard drive is very real.

Digital rights management systems and watermark encryption are recent technologies that may prevent unauthorized exchanges of protected files in the future. Some of these technologies have already been used to prevent the unauthorized distribution of Microsoft XP, computer games, and files sold by new music download technologies such as Apple's iTunes.[283] Nevertheless, there are still significant hurdles for these technologies to overcome. First, like all digital

---

[281] Landau, *supra* note 4, at 435.
[282] *Id*. at 435-36.
[283] Mike Langberg, *Apple Rocks on with iTunes*, SILICONVALLEY.COM, Oct. 23, 2003, *at* http://www.siliconvalley.com/mld/siliconvalley/business/technology/personal_technology/7082855.htm.

technologies, copy protection devices are inevitably prone to hacker circumvention. Second, companies must be wary against implementing anti-circumvention devices that make a product unattractive to consumers. For example, Sony suffered a significant amount of consumer backlash after unveiling plans to release copy-protected CDs containing content that can only be copied from a computer to a Sony portable player.[284]

Finally, these technologies must adequately deal with users' fair use rights. Copy protection devices that fail to allow *any* copying, even by authorized users, may run counter to a consumer's expectation to make fair use of the product. Although the Supreme Court has never held that fair use is constitutionally required, the Court has noted that "*some opportunity for fair use of copyrighted materials has been thought necessary to fulfill copyright's very purpose*."[285] Copyright holders, however, might argue that "fair use" merely gives consumers the expectation to make *a* fair use copy, and not necessarily a copy of the highest quality. Thus, it could be argued that simply tape-recording a CD would satisfy a consumer's fair use expectation.

2. Contractual Copying

If digital rights management systems are able to survive in the face of hackers and disillusioned consumers, contractual copying may become a viable solution. Under this proposal, companies would set up different price points for a download depending upon the number of "usages" allowed.[286] For example, iTunes could offer downloads that allow one file transfer for 20 cents, two file transfers for 40 cents, and so on. Accordingly, if a consumer wishes to download a file and make four fair use copies, he will have to pay a higher price than if he does not wish to make any secondary copies at all. Although this system may solve the problem of fair use (albeit, at a price), companies must still find a way to prevent consumers from simply paying the higher price for the ability to upload the file to a free peer-to-peer network.

Nevertheless, contractual copying systems may also be disadvantageous to consumers. Companies may take into account the "peer-to-peer value" of downloads and charge consumers more for the

---

[284] Jay Lyman, *Sony Attempts New Copy-Protection* Strategy, E-COMMERCE TIMES, Nov. 11, 2003, *available at* http://www.ecommercetimes.com/perl/story/32111.html.
[285] Campbell v. Acuff-Rose Music, Inc., 510 U.S. 569, 575 (1994). *See also* Universal City Studios, Inc. v. Corley, 273 F.3d 429 (2d Cir. 2002).
[286] Landau, *supra* note 4, at 439.

added "uses" of music downloads, such as uploading the file to a free peer-to-peer network. The threat of consumers defecting to a free peer-to-peer service, however, may also help keep prices reasonable.

3. The Potential AHRA Conflict

It is unclear whether the language of the AHRA *allows* consumers to make lawful digital copies, or merely immunizes them from liability.[287] If the former interpretation is correct, copyright holders may be prohibited from attaching technological devices that prevent consumers from making digital copies. Even if the AHRA merely immunizes consumers who make personal copies, copyright holders who do not allow consumers to copy their works would most likely be precluded from collecting the royalties mandated by the AHRA.[288] More importantly, the AHRA does not currently include computers or their hard drives under its definition of a digital copying technology. One possible solution is to amend the AHRA to explicitly include computers as a copying device. As a result, computer manufacturers would have to pay copyright holders royalties for the digital copying of their works.[289] Copyright holders, however, might argue that the royalties are disproportional to the financial loss brought about by online file sharing. Furthermore, computer manufacturers (and ultimately consumers) would undoubtedly disagree with such a costly proposal.[290]

Although digital rights management systems may hold the key to solving the peer-to-peer conflict, these technologies are still years away from perfection. Until then, other possible remedies must be considered.

C. Education

In September of 2002, Music United for Strong Internet Copyright (MUSIC) launched a campaign designed to educate consumers about both the illegality and harm caused by unauthorized file sharing.[291] High-profile musicians such as Britney Spears, Madonna, and Elton John appeared in radio and television commercials to speak out against the harms of piracy.[292] Furthermore, the Copyright Society of the USA

---

[287] Norman, *supra* note 2, at 407.
[288] *See* Colletti, Jr., *supra* note 11, at 260.
[289] Landau, *supra* note 4, at 441.
[290] *Id*.
[291] Norman, *supra* note 2, at 403.
[292] *Id*.

created "Copyright Awareness Week" in 2002, a "yearly event directed at school-age children . . . (that) offered teachers handouts and lesson plans for the week for children of all ages."[293]

Copyright holders are ostensibly relying on the theory that consumers do not realize the illegality of file sharing; thus, if these consumers learn that their behavior is unlawful, they will stop downloading copyrighted files. The recent decline in traffic on high-profile peer-to-peer networks may be evidence that this theory has some merit.[294]

Nevertheless, while education may have an effect upon young children who download copyrighted material, it is highly doubtful that a substantial percentage of adult downloaders fail to realize the illegality of their conduct. High-profile decisions such as *Napster* and *Grokster* were mainstream news-fodder; the peer-to-peer conflict has been continually featured in newspapers and nightly news broadcasts on major broadcast stations. More to the point, very few adult file-sharers are not aware that receiving copyrighted material for free is *illegal*. I suggest that peer-to-peer users continue to download copyrighted material for three reasons entirely unrelated to lack of education: (1) they enjoy the benefits of "something-for-nothing," and do not fear being caught; (2) they believe that they have already paid their dues to the RIAA by purchasing CDs, and download unauthorized material merely because it is an easy method for sharing their music with distant friends or replacing destroyed CDs; and (3) they believe the cost of music is far too high, and believe they are "getting even" for years of unwarranted price-hikes and inflated CD prices. Of these suggestions, I believe that the first and third are the most probable explanations.

Therefore, educational campaigns featuring wealthy artists are unlikely to gain much sympathy from the average consumer. I highly doubt that the average consumer, struggling to make ends meet, will shed many tears for the financial losses of Elton John or the RIAA. Furthermore, the RIAA lost any possible chance of winning consumer empathy when they launched the rather daft strategy of filing lawsuits against consumers themselves. To most consumers, the copyright conflict is the modern-day story of Robin Hood: the peer-to-peer networks represent Robin Hood, while the recording industry portrays the Sheriff of Nottingham.

RIAA president Hillary Rosen recently claimed, "[o]ur analysis shows that there's still a significant percentage of people (who do not

---

[293] *Id*.

[294] Alsever, *supra* note 214.

realize) it's illegal, and when they do, they are willing to change their behavior."[295] Rosen's statement is yet another example of the RIAA acting as an ostrich, head firmly planted deep in the sand. Until large-scale copyright holders acknowledge the *real* reasons for the prevalence of illegal downloading, expenditures on national educational campaigns concerning the "harms" of file sharing constitute a complete waste of resources and capital.

So what are the *real* causes of illegal downloading, and how can the music industry devise a solution? I propose that the answer to both questions can be found in the legal market for music sales.

D. Market Correction: How Better Business Practices can Save the Music Industry

"Go on and save yourself" – Audioslave

Many consumers simply dislike the idea of paying $17.00 for a compact disk that cost less than a dollar to produce. Further compounding the problem is the fact that many compact disks contain only a handful of palatable songs. Thus, the pattern is as follows: a consumer hears a song on the radio; the consumer purchases that artist's CD for $17.00; the consumer dislikes most of the other songs on the album, and therefore realizes he paid $17.00 for the right to listen to one or two songs. Although this is an extreme generalization, the general principle of consumer dissatisfaction with the recording industry has played a substantial part in the rise of free peer-to-peer technology.

1. Compact Discs

The recording industry has two options with regard to increasing sales of compact disks: (1) lower the cost of CDs to a price consumers are willing to pay, or (2) keep the prices the same, but offer additional material on the CD.

DVD manufacturers have already embraced the latter option. DVDs now commonly include additional scenes, director commentary, games, and other hard-to-find materials alongside the movie itself. As a result, DVD sales have flourished. Some CD manufacturers have begun taking notice, and have included live footage and music videos alongside an artist's album. These "bonus materials," however, are usually either

---

[295] Norman, *supra* note 2, at 404.

included on a separate disk, or reflected in the higher price of a single disk. The recording industry may also try to attract the more "fanatical" music fan by "distinguishing the physical entertainment package" and "adding lyrics, posters, and other bonuses to entice fans to purchase the tangible object."[296]

The recording industry has been reluctant to lower the price of CDs, citing the high costs of artist development, artist retention, and greedy music publishers.[297] The retail prices of CDs "has increased by approximately 50% over the last several years."[298] The recent decline in music sales is a sign that consumers are simply no longer willing to pay outrageous prices to own a piece of music. Nevertheless, the online world has made it possible to reduce the cost of music to the *exact* price consumers are willing to pay.

In the real world, a CD will be released at a "high" price, and consumers who wish to own the new music immediately must pay that premium.[299] After initial sales lag, the price is often lowered with the hopes that additional consumers will agree to purchase the CD at a reduced price.[300] Finally, when little consumers interest remains in a CD, the price is lowered to the "bargain basement" level.[301] Thus, there are a finite number of "price points" a CD touches upon during its lifespan.

Online digital rights management systems, however, enable a CD to be priced at an almost infinite number of price points. For example, on the first day a song is released, consumers may be willing to pay $2.00. The next week, consumers may only be willing to pay $1.80; therefore, CD sales will lag at the $2.00 level. In the real world, it is impossible to manually re-label the price of all CDs in circulation to the correct price point. In the online world, Internet music stores can quickly and efficiently lower their prices almost daily, thereby tailoring a song's price point to the exact amount a consumer is willing to pay. Thus, a song can simply be sold for $2.00 one day, $1.99 the next day, and so on until consumers are only willing to pay a nickel for it. Similarly, users can pay different fees depending upon the number of uses/copies they wish to make of a song. In this way, the Internet provides a unique

---

[296] *Id*. at 408-09.
[297] *Id*. at 402.
[298] Landau, *supra* note 4, at 441.
[299] *See* Joanna Tamer, *The Channel Watch; And Digital Media*, 428 PLI/Pat 17, 19 (1996).
[300] *Id*.
[301] *Id*.

medium for bridging the gap between consumers and the recording industry.

2. Peer-to-Peer Competition

Nevertheless, even with the new age of digital market economics upon us, cynics argue, how can the recording industry effectively compete with networks that offer material for *free*? The answer is simple: make it worth their while to pay for it.

Most people own cars. All cars need an oil change at least twice a year. Barring physical disability, any car owner who possesses a socket wrench can change his oil. The act itself is not difficult: reach under a car, remove the bolt, let the old oil filter out into a pan, replace the bolt, refill the car with new oil, and dispose of the old oil at a local Wal-Mart. In fact, the entire operation takes 15 minutes. Nevertheless, most people pay approximately $15 to $20 dollars for a mechanic to do it. People have busy schedules and dislike devoting a half-hour of their free time to automobile maintenance. It is simply more *convenient* for someone else to do it.

Similarly, it takes the average peer-to-peer user anywhere from one minute to an hour to download a single song. In fact, depending upon the speed of a user's server and the time of day they are downloading the file, it can take even longer. Furthermore, a user may unwittingly download an incomplete song (or the wrong song entirely) and be forced to re-start the process anew. Of course, the above scenario only relates to users who are lucky enough to locate the desired song on their peer-to-peer network to begin with.

Therefore, a peer-to-peer user may be more than willing to pay a small fee for the *convenience* of downloading a song at a fraction of the time and hassle. If the recording industry can effectively utilize pay-per-use digital technology, they may be able to beat the decentralized peer-to-peer systems at their own game.

3. If You Can't Beat Them, Join Them: Legalized File Sharing

Before the Supreme Court's decision in *Sony*, the movie industry argued that a ruling for Sony would result in major financial losses for major studios. History, however, tells a different story: *Sony* sparked the movie industry to become involved in the home-video market, which created a powerful new source of revenue that is still paying dividends

for the motion picture industry. In fact, the *Sony* decision not only failed to irreparably damage the incentive to create motion pictures, but actually increased it: pictures that would have been previously shunned by theatres now enjoy a new financial life in the market niche of "straight-to-video" movies. The RIAA has already begun a similar strategy with the release of legal download services such as iTunes and Musicmatch.

Online music sales have been increasing at a phenomenal rate. In 2002, consumers spent $16 million on Internet music; in 2003, about $50 million.[302] Legal pay-per-use systems offer many incentives for consumers to switch over from decentralized peer-to-peer sites such as Kazaa and Grokster.

First, these sites are *legal*. Consumers who switch over to the legal sites need no longer worry about facing a $2,500 settlement for downloading their favorite song. Furthermore, consumers who are disillusioned with buying a $17.00 CD for a handful of decent songs need worry no longer; the new legal download sites enable consumers to purchase songs individually for less than a dollar each.

Second, legal download sites can potentially offer much faster searches and downloads than decentralized networks. Consumers may be more than willing to pay a few cents for the *convenience* of owning a song almost instantly. Also, unlike decentralized networks, consumers can be certain that they know what they are downloading; the decentralized problems of viruses and corrupted files do not generally exist on legal download sites. Consumers also need not worry about excessive "Adware" that produces "pop-up ads, privacy violations and crashed computers," a problem that exists on most decentralized sites.[303]

Finally, the interfaces of the legal download sites are generally simple in design and easy to use when compared with the relatively complicated decentralized interfaces. On a whole, the quality of the music is better as well. Furthermore, licensing agreements between the major recording companies have given sites such as Napster 2.0 and iTunes a vast selection of music to choose from.[304]

However, problems still exist. The selection of music on decentralized peer-to-peer networks is far greater than that of any particular legal download site. Some legal download sites, particularly Musicmatch and Rhapsody, have been prone to bugs.[305] Nevertheless,

---

[302] Cave, *supra* note 216, at 16.
[303] Damien Cave, *Free Music,* ROLLING STONE, Feb. 5, 2004, at 16.
[304] Cave, *supra* note 216, at 16.
[305] *Id*. at 17.

legal download sites are still in their infancy. If utilized correctly by the recording industry, these sites have the potential to provide significant competition to free peer-to-peer sites, and perhaps eventually provide the solution to the peer-to-peer conflict.

VI. CONCLUSION

If the peer-to-peer conflict has proven anything, it is that there is no easy way to balance artists' incentive to create and the rights of the public. Nevertheless, when the rights of copyright holders and the public come into conflict, the benefit should be given to the public interest. It is important for the courts, the legislature, and copyright holders to realize that peer-to-peer networks are not exclusively used for the illegal exchange of copyrighted material. These networks offer a variety of services to the public, and may revolutionize the way information is exchanged in the near future.

The RIAA's members and other large-scale copyright holders must begin fighting the copyright war the right way by developing new technologies and utilizing existing peer-to-peer technologies to effectively compete with illegal file sharing. They must realize that the spread of Internet piracy is largely a result of their own suspect business decisions. In sum, large-scale copyright holders must stop claiming they are victims of decentralized peer-to-peer technology. If copyright holders focus less on lawsuits and more on better business practices, a satisfactory solution to the peer-to-peer problem may be looming just over the horizon. Nevertheless, if copyright holders continue their negative, senseless attacks upon new technologies and the consumers who use them, the war over decentralized peer-to-peer technologies will continue to be waged for years to come.