Peer-to-peer Distribution Systems: Will Napster, Gnutella, and Freenet Create a copyright Nirvana or Gehenna?

Damien A. Riehl

Follow this and additional works at: http://open.mitchellhamline.edu/wmlr

Recommended Citation
Available at: http://open.mitchellhamline.edu/wmlr/vol27/iss3/1

This Article is brought to you for free and open access by the Law Reviews and Journals at Mitchell Hamline Open Access. It has been accepted for inclusion in William Mitchell Law Review by an authorized administrator of Mitchell Hamline Open Access. For more information, please contact sean.felhofer@mitchellhamline.edu.
© Mitchell Hamline School of Law
# PEER-TO-PEER DISTRIBUTION SYSTEMS: WILL NAPSTER, GNUTELLA, AND FREENET CREATE A COPYRIGHT NIRVANA OR GEHENNA?

Damien A. Riehl†

<table>
<thead>
<tr>
<th>Section</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>I. INTRODUCTION</td>
<td>1762</td>
</tr>
<tr>
<td>II. DESCRIPTION OF PEER-TO-PEER SYSTEMS</td>
<td>1764</td>
</tr>
<tr>
<td>III. NAPSTER</td>
<td>1766</td>
</tr>
<tr>
<td>A. Introduction</td>
<td>1766</td>
</tr>
<tr>
<td>B. Napster's Software Architecture</td>
<td>1768</td>
</tr>
<tr>
<td>C. A &amp; M Records, Inc. v. Napster, Inc</td>
<td>1768</td>
</tr>
<tr>
<td>1. “Safe Harbor” Provision Of The DMCA</td>
<td>1769</td>
</tr>
<tr>
<td>2. Napster's Argument Under Sony Corp. Of America v. Universal Studios</td>
<td>1770</td>
</tr>
<tr>
<td>3. Preliminary Injunction And Stay Pending Appeal</td>
<td>1771</td>
</tr>
<tr>
<td>4. Traceability Of MP3 Files</td>
<td>1772</td>
</tr>
<tr>
<td>IV. GNUTELLA</td>
<td>1773</td>
</tr>
<tr>
<td>A. Introduction</td>
<td>1773</td>
</tr>
<tr>
<td>B. Gnutella's Software Architecture</td>
<td>1775</td>
</tr>
<tr>
<td>C. Legal Implications</td>
<td>1776</td>
</tr>
<tr>
<td>V. FREENET</td>
<td>1779</td>
</tr>
<tr>
<td>A. Background</td>
<td>1779</td>
</tr>
<tr>
<td>B. System Architecture</td>
<td>1781</td>
</tr>
<tr>
<td>C. Legal Implications</td>
<td>1782</td>
</tr>
<tr>
<td>1. Anonymity For Producers And Consumers</td>
<td>1782</td>
</tr>
<tr>
<td>2. Deniability For Users Who Store Information</td>
<td>1783</td>
</tr>
<tr>
<td>3. Resistance To Third-Party Attempts To Deny Access</td>
<td>1785</td>
</tr>
<tr>
<td>4. Efficient Storage And Routing</td>
<td>1785</td>
</tr>
<tr>
<td>5. Decentralization Of Network Functions</td>
<td>1786</td>
</tr>
<tr>
<td>VI. SOLUTIONS FOR PEER-TO-PEER NETWORKS</td>
<td>1787</td>
</tr>
<tr>
<td>A. Legislative Remedies</td>
<td>1787</td>
</tr>
<tr>
<td>B. Technological Remedies</td>
<td>1789</td>
</tr>
</tbody>
</table>

† J.D. Candidate 2002, William Mitchell College of Law; B.S., North Dakota State University, 1997. Author may be contacted at driehl@wmitchell.edu.
"Freedom and not servitude is the cure for anarchy; as religion, and not atheism, is the true remedy for superstition."

I. INTRODUCTION

Since its inception, American copyright law has been at odds with "new use" technologies that periodically threaten to eliminate a content owner's ability to enforce her copyright. Initially, these new uses seem to be the death knell to copyright protection, but in nearly every instance copyright law has adjusted to the new use—often creating an unexpected and lucrative source of revenue for the copyright holders that had initially been so opposed to its introduction. Examples of such historically threatening technology include piano rolls, phonographs, motion pictures, cable television, photocopiers, videocassette recorders ("VCRs"), and Digital...
Audio Tapes ("DATs").

The Internet is merely the newest entrant in the battle between copyright-holders' interests in compensation and the consumer's interest in accessing copyrighted content in an unprecedented manner. High-profile lawsuits, such as those involving MP3.com and Napster, have forced the courts, Congress, copyright owners, and the American public to question the manner in which we can preserve the concept of copyright on the Internet. Most of these cases have dealt with legality of offering musical recordings in MP3 format, but the underlying issue—how to adapt the law to conform with the capabilities that a new medium can offer—applies to any type of copyrighted content.

Peer-to-peer systems present additional legal difficulties not addressed by litigation involving their Internet counterparts. The largest of these questions are ascertaining jurisdiction and narrowing down a defendant. Prior and current defendants in Internet

17 U.S.C.A. § 1 et seq.).
8. E.g., Williams & Wilkins Co. v. United States, 487 F.2d 1345, 1359 (Ct. Cl. 1973), aff'd 420 U.S. 376 (1975) (holding that a medical journal publisher's photocopying is considered a "fair use" because it is a nonprofit institution devoted to the advancement of medical knowledge).
9. E.g., Sony Corp. of Am., 464 U.S. at 417.
14. MP3 is the common name for the audio compression standard, otherwise known as MPEG Audio Layer 3, or Moving Picture Experts Group, Audio Layer 3. Recording Indus. Ass'n of Am. v. Diamond Multimedia Sys. Inc., 180 F.3d 1072, 1074 (9th Cir. 1999). Where digital music files have traditionally been large and difficult to transmit in means other than by compact disc, MP3 compression technology eliminates from a recording most sounds not detectable by the human ear, thereby decreasing file size to one-twelfth of the original. Id. The smaller file size makes transmission over the Internet much faster and facilitates storage in portable devices such as the Diamond Rio. See generally Lisa M. Needham, A Day in the Life of the Digital Music Wars: The RIAA v. Diamond Multimedia, 26 WM. MITCHELL L. REV. 1135 (2000).
copyright infringement cases have usually been individuals or corporations, each of them being a single, identifiable entity. These types of potential defendants make narrowing down the target of a lawsuit relatively easy to determine. If a defendant's distribution method is deemed to be an infringement of copyright in these cases, a court may award damages, an injunction, or both. In the last two systems analyzed in this article, however, the allegedly offending system is not one entity or company that a plaintiff could sue, but it is merely a network protocol that could be used by millions of private individuals all over the world. Without a central presence, a plaintiff may have a difficult time enforcing an injunction against millions of users who are spread throughout the world. The proliferation of peer-to-peer systems require us to rethink the legal methods we are using to protect the concept of copyright.

II. DESCRIPTION OF PEER-TO-PEER SYSTEMS

Peer-to-peer systems are reminiscent of the beginnings of the Internet, which began as a network designed by the military to be used for communication in case of nuclear war. With this purpose in mind, it was designed to maintain its integrity even if a portion of the Internet would fail. The military created a decentralized structure that allowed each user to both send and receive information with another user without having to go through an intermediary server.

As the Internet matured and became more commercialized, it moved away from users directly communicating with each other and evolved into a series of spokes and hubs. Each "hub" is a server computer on which web sites and other information are stored. Each user accesses this information from her personal

15. Supra text accompanying notes 13 and 14.
16. The system, called ARPANET, was developed in 1969 through the efforts of the military and other universities doing military defense. Reno v. ACLU, 521 U.S. 844, 849-50 (1997).
17. Id.
18. "The ARPAnet became the first computer network in the nation, and in it, each computer was an equal partner. That 'peer-to-peer' concept remains the fundamental idea in networking." John Markoff, Creating a Giant Computer Highway, N.Y. TIMES, Sept. 2, 1990, at 1.
computer through "spokes" connecting her to those servers.\textsuperscript{20}

In contrast, Napster and other peer-to-peer systems are returning to the origins of the Internet by allowing every user to be both a spoke and a hub—allowing the dissemination and receipt of information simultaneously, creating a peer-to-peer ("P2P") network.\textsuperscript{21} Essentially, each user's computer becomes a server itself, obviating the need for large, expensive servers to distribute information to other users.\textsuperscript{22} While each user is uploading information to another user, she may also download information from other users connected to this system.\textsuperscript{23}

Napster's introduction in November 1999 not only expanded the manner in which users may share music, but it also reminded the Internet developers of the power of peer-to-peer technology.\textsuperscript{24} One area that may be affected by the renaissance of peer-to-peer systems is the manner in which we search the Internet. Currently, if someone would like to find information on the Internet, she logs onto a search engine such as AltaVista or Google that periodically indexes text on a catalog of sites. When a user initiates a search, the search engine looks through sites contained in its catalog and returns the results of the search to the user.\textsuperscript{25} Those results may be outdated, since the engines only periodically review and re-index the sites in their catalog. Peer-to-peer networks provide the capability to provide "real time" searches.\textsuperscript{26} With the advent of Napster

\begin{itemize}
\item \textsuperscript{20} Id.
\item \textsuperscript{22} Id. See also infra note 39 (representing the operation of Napster).
\item \textsuperscript{23} Streitfeld, supra note 21.
\item \textsuperscript{24} Netscape co-founder Marc Andreessen has said that the introduction of peer-to-peer systems “changes the Internet in a way that it hasn’t changed since the browser.” Ariana Eunjung Cha, E-Power to the People; New Software Bypasses Internet Service Providers, WASH. POST, May 18, 2000, at A01, available at 2000 WL 19609619.
\item \textsuperscript{25} A report by BrightPlanet (http://www.brightplanet.com/) reported that even the most comprehensive search engines, such as Google.com, only analyze about one billion of the world’s 550 billion web sites. Elizabeth Weise, One Click Starts the Avalanche: Buried in Information? Smarter Searching Comes to the Rescue, USA TODAY, Aug. 8, 2000, at 3D, available at 2000 WL 5786161; BrightPlanet, The Deep Web: Surfacing Hidden Value, available at http://128.121.227.57/download/deepwebwhitepaper.pdf, at iii (last visited Jan. 4, 2000).
\item \textsuperscript{26} Gnutella developer Gene Kan has founded a company called Gonesilent.com to build InfraSearch, a search engine based upon the peer-to-peer system, Gnutella. Netscape co-founder Marc Andreessen is an investor in the company, which plans to search websites that have been previously unavailable because
\end{itemize}
and other peer-to-peer networks, every site on the Internet could be connected and indexed with up-to-the-second results.\footnote{27}

Napster, Gnutella, and Freenet are three systems that have demonstrated the power of peer-to-peer distribution, and each has characteristics that make it difficult to enforce copyright law as it is now composed. If we are to be successful in maintaining the integrity of copyright law, we must become familiar with the structure of the systems to ascertain ways in which the copyright law can be adapted to fit these new uses.

III. NAPSTER

A. Introduction

Napster is a file-sharing application that was conceived by a college student who wanted to easily share songs over the Internet with his friends.\footnote{28} It was introduced to the public in November 1999, and it has grown to become an Internet giant—backed by millions of dollars in venture capital\footnote{29} and more than 40 million us-


\footnote{27} Id.


\footnote{29} As of July 30, 2000, Napster had raised $17.5 million in venture capital, and lead attorney, David Bois has stated that he believes Napster's worth to be somewhere between $800 million and $1.5 billion. \textit{Napster Has Struck a Major Chord}, MILWAUKEE J. & SENTINEL, July 30, 2000, at 25D, available at 2000 WL 3872902. Though it does not currently charge for its services, technology venture capitalists have invested in Napster, apparently under the premise that it will conceive of a way to generate revenue in the future and that peer-to-peer networks will become a new Internet standard. Michael Liedtke, \textit{No Going Back Technology: Entrepreneurs Say, Regardless of Napster's Fate, the Peer-To-Peer Computing Concept Can't Be Put Back in the Tube}, ORANGE CNTRY. REG., JULY 28, 2000, at C01, available at 2000 WL
In September 2000, Napster users shared 1.39 billion songs, and there were about one million users on the system at any given time. Napster estimated that it would have more than 75 million users by the end of the year 2000, and the program has been installed on approximately thirty percent of personal computers.

Much of the attention surrounding Napster has been attributed to high-profile cases involving the Recording Industry Association of America ("RIAA") and other well-known music artists, which have thrust Napster into the national spotlight. The notoriety of these cases has also placed Napster in the center of an ongoing debate over how copyright law should coexist with the continued evolution of the Internet.

---


37. Heavy-metal group Metallica, Metallica et al. v. Napster Inc. et al., No. 00-0391, complaint filed (C.D. Cal., Apr. 13, 2000), and rapper Andre Young ("Dr. Dre"), Young et al. v. Napster Inc. et al., No. 00-04366, complaint filed (C.D. Cal., Apr. 25, 2000), have filed separate suits against Napster for allegedly enabling others to infringe upon their copyrights. Christopher Jones, Metallica Rips Napster, WIRED NEWS (Apr. 13, 2000) at http://www.wired.com/news/print/0,1294,35670-0,00.html.

38. See generally Karl Taro Greenfeld, Meet The Napster: Shawn Fanning Was 18 When He Wrote the Code That Changed the World. His Fate, And Ours, is Now in the
B. Napster’s Software Architecture

When a user logs on to Napster, she uses Napster’s proprietary MusicShare software to connect to one of Napster’s central servers. After the user connects, the server catalogs the user’s MP3 files and makes the names of the files available to other Napster users. A user may then use the MusicShare software to search other users’ computers for a specific song or artist, whereby a list is generated, showing the files available for download. To download a song, the user merely highlights a song, clicks the “Get Selected Song(s)” button, and the song is transferred from the host user’s computer to the requesting user’s computer.


In December 1999, the Recording Industry Association of America (“RIAA”) filed suit against Napster, alleging both con-


39. A & M Records, Inc. v. Napster, Inc., 114 F. Supp. 2d 896, 905 (N.D. Cal. 2000). Appendix Diagram A, created by the author, gives a pictorial demonstration of Napster’s operation: (1) Napster server collects listing of host computer’s MP3s; (2) Requesting user queries Napster catalog to see if MP3 is available on another user’s computer; (3) If host computer has the MP3, the Napster server will show the requesting user which host computer has the file; (4) The requesting user contacts the host computer directly, and (5) downloads the file from the host computer.

40. Id.

41. Id. at 905-06.

42. Id. at 906. With increasing availability of broadband services such as Digital Subscriber Lines (“DSLs”) and cable modems, the music industry has been justifiably concerned. Depending upon the user’s connection speed to the Internet, a ten megabyte (“10 MB”) song may be downloaded in as little as one minute. Downloading that same song using a fifty-six kilobit per second (“56K”) modem would take twenty-four minutes, while a ten megabit per second (“10 Mb/s”) cable modem it would only take eight seconds to download. Sharon Watson, Bandwidth Booster, INTERNET TELEPHONY, (Oct. 6, 1997) at http://www.internettelephony.com/archive/10.06.97/cover.html; 2000 WL 1032533.


tributory infringement of copyrights and vicarious infringement of copyrights. In its complaint, the RIAA averred that illegal copies of the songs traded using the Napster service would not have been as widely available were it not for Napster. Further, they argued that Napster refused to maintain a database of users and infringing files, though it had the right and obligation to do so. The RIAA argued that because of this purposeful ignorance, Napster was vicariously liable for the alleged copyright infringements taking place on its service.

1. "Safe Harbor" Provision Of The DMCA

Napster filed a motion for summary judgment, arguing that it falls under the protection of the "safe harbor" provision of the Digital Millennium Copyright Act, which limits liability for service providers.

Napster argued that it is a "service provider" under 17 U.S.C. § 512(k)(1)(A), which defines "service provider" as "an entity offering the transmission, routing, or providing of connections for digital online communications, between or among points specified by a user, of material of the user's choosing, without modification to the content of the material as sent or received." Napster contended that it is merely a "passive conduit" for the information and is thus entitled to the protections allowed to service providers under the DMCA section 512(a).

45. Contributory copyright infringement refers to "one who, with knowledge of the infringing activity, induces, causes or materially contributes to the infringing conduct of another, [and who] may be held liable as a 'contributory' infringer." Sony Corp. Am. v. Universal City Studios, Inc. 464 U.S. 417, 487 (1984) (quoting Gershwin Publ'g Corp. v. Columbia Artists Mgmt., Inc., 443 F.2d 1159, 1162 (2d Cir. 1971)).

46. Vicarious infringement of copyright refers to when one "has the right and ability to supervise the infringing activity and also has a direct financial interest in such activities." Fonovisa, Inc. v. Cherry Auction, Inc., 76 F.3d 259, 262 (9th Cir. 1996) (quoting Gershwin, 443 F.2d at 1162).

47. Napster Complaint at ¶ 57.
48. Id. at 67.
49. Id. at 70.
Plaintiffs, however, argued that 512(a) did not apply since the allegedly infringing material did not go "through" the Napster servers, but was transmitted directly between users' machines. Further, they argued that each section of the DMCA must be analyzed independently and that the more narrow subsection 516(d), which refers to information location tools such as search engines, is more applicable to Napster. The court ultimately agreed with the RIAA, rejecting Napster's 512(a) "safe harbor" argument and ruling that Napster neglected to curtail copyright infringement in accordance with 512(i).

2. Napster's Argument Under Sony Corp. of America v. Universal Studios

The RIAA next filed a Motion for Preliminary Injunction to force Napster to cease its activities pending the outcome of the trial. In this motion, the RIAA argued that the "tens of millions of

*N (N.D. Cal. 2000). Section 512(a) of the DMCA states in part that "[a] service provider shall not be liable for monetary relief ... or other equitable relief, for infringement of copyright by reason of the provider's transmitting, routing, or providing connections for, material ... or by reason of the intermediate and transient storage of that material ...." Actions fall under this provision if (1) the initiation of the transmission was not directed by someone other than the ISP, (2) the transmission is automatic, (3) the ISP does not select the recipient, (4) no copies are maintained on the ISP server, and (5) material is transmitted through the server without modification. 17 U.S.C. § 512(a)(1-5)(1998).

54. Supra note 39.
55. *Id.* 2000 WL 573136, at *6-7.
57. *Id.* Section 512(d) of the DMCA states that an ISP that links to infringing material is protected if, *inter alia*, it does not know that the material is infringing, it should not know that the material is infringing, it quickly removes or disables access to the material, and it does not financially benefit from the activity. 17 U.S.C. § 512(d) (1) (A)-(C), (2)(1998).
59. *Id.* at *10. Section 512(i) limits liability for service providers only if the provider "has adopted and reasonably implemented, and informs subscribers and account holders of the service provider's system or network of, a policy that provides for the termination in appropriate circumstances of subscribers and account holders of the service provider's system or network who are repeat infringers...." 17 U.S.C. § 512(i) (A) (1998).
61. RIAA Notice of Joint Motion and Joint Motion of Plaintiffs for Preliminary Injunction; Memorandum of Points and Authorities, A & M Records, Inc. v.
copies of copyrighted music” transferred using Napster inflicted irreparable harm upon the RIAA.  

This phase of the litigation saw Napster’s first attempt to invoke the U.S. Supreme Court decision in *Sony Corp. of America v. Universal Studios*, which held that “the sale of copying equipment ... does not constitute contributory infringement if the product is widely used for legitimate, unobjectionable purposes. Indeed, it need merely be capable of substantial noninfringing uses.” Citing *Sony*, Napster argued that it is capable of “numerous and substantial non-infringing uses” and should have no liability in the current litigation.  

3. Preliminary Injunction And Stay Pending Appeal

The trial court granted the RIAA’s Motion for Preliminary Injunction at the end of the hearing, finding that the RIAA had a “strong likelihood of success on the merits” regarding the vicarious and contributory liability claims. It rejected Napster’s affirmative defense regarding *Sony* and the fair use doctrine.  

In an unanticipated bench decision, the court ruled that Napster was prohibited from “causing or assisting or enabling or facilitating or contributing to the copying, duplicating or ... other infringement upon all copyrighted songs, musical compositions or material in which plaintiffs hold a copyright or with respect to plaintiffs’ pre-1972 recordings in which they hold the rights.” Thus, Napster was not required to shut down, but it must merely devise a way to keep infringing files off the system. The court noted that the intelligent people who created Napster should be able to find a way to block any infringing files. The injunction was

---

62. *Id.* at 925.  
64. *Id.* at 442.  
67. *Id.* at *5.  
68. *Id.* at *8.  
69. *Id.*  
70. *Id.* at *6. From the bench, Judge Patel said that she was “sure that anyone
to take effect two days later at midnight on Friday, July 28.\textsuperscript{71}

Napster filed a Motion for Stay Pending Appeal with the Ninth Circuit Court of Appeals,\textsuperscript{72} which granted the motion hours before the injunction was to be enforced.\textsuperscript{73} The Ninth Circuit heard oral arguments regarding the injunction on October 2, 2000.\textsuperscript{74} During the oral argument, the panel focused upon Napster's ability to identify copyrighted files on its system and its duty to block those infringing files from its service.\textsuperscript{75} One justice thought that it was "extremely troublesome" that the RIAA wanted the court to hold Napster responsible for the actions of its users.\textsuperscript{76} One member of the panel grilled the RIAA about the feasibility of overcoming jurisdictional hurdles by asking, "How are they expected to have knowledge of what comes out of some kid's computer in Hackensack, N.J., and is transmitted to Guam?"\textsuperscript{77}

4. Traceability Of MP3 Files

There has been a significant amount of discussion as to whether Napster can, as Judge Patel suggested,\textsuperscript{78} track illegal trading of copyrighted songs. Other independent sources have argued that Napster would be able to identify copyrighted material by analyzing the hash marks found on every MP3 file.\textsuperscript{79} The digital fin-


\textsuperscript{77} \textit{Id.}

\textsuperscript{78} Napster, 2000 WL 1009483, at *6.

\textsuperscript{79} Charles C. Mann and Roger Parloff, \textit{Napster Playing Dumb, Experts Say: Programmers Say the Company Could Easily Block Most of the Infringing Files From Its Direc-
gerprint, termed an "MD5 hash," uniquely identifies an MP3 file that has been recorded under identical conditions and recording speed. 80 The RIAA has contended, and at least one source has confirmed, that a majority of copyrighted songs can be identified and removed from the Napster system by filtering files according to MD5 configurations. 81

Digital music retailer Emusic has installed a system that it purports will scan Napster using MD5 hash configurations to identify songs that have been distributed on its system. 82 If the system confirms that a Napster user is sharing files that have been downloaded from Emusic’s site, the system will notify the user that the materials must be removed from Napster within twenty-four hours or Napster will block the user’s account. 83 If the system is successful in identifying infringing files, they will have effectively done what Napster has insisted is unfeasible: identifying infringing files upon the Napster system. 84

IV. GNUTELLA

A. Introduction

Gnutella 85 is another example of peer-to-peer software capable of being a thorn in the sides of the entertainment industry and

80. Id. NetPD, the company that assisted Metallica in its search for infringing files, conducted a six-month study that found that most of the files on the Napster network were originally ripped from relatively few sources, so they had identical MD5 characteristics. Id. Only ten MD5 hashes accounted for more than eighty-five percent of a three-song test sample. Id.


83. Id.

84. Id.; supra note 70.

85. Gnutella is located at http://gnutella.wego.com/ (last visited Jan. 10, 2000). Pronounced NEW-tella, the name is a combination of the “GNU” open-source operating system upon which the program was written, and “Nutella,” the hazelnut and chocolate spread. Lianne George, Gnutella: The Future of Online Music?, TORONTO STAR, July 27, 2000 at FF05, available at 2000 WL 24060441; Adam Pasick, Free for All—For Now: Gnutella Ups the Ante When it Comes to Sharing Pirated Files, ZDNET (June 14, 2000) at http://www.zdnet.com/special/stories/collegeguide/0,11234,2576235,00.html.
other copyright owners. Though it is similar to Napster, it is more problematic in that it does not have a centralized server system, but instead connects its users with each other directly without using an intermediary.

Gnutella was written by Justin Frankel, creator of Winamp, while he was an employee of Nullsoft, a subsidiary of America Online ("AOL"). Frankel wrote the program in his bedroom and posted it on the AOL site without asking AOL's permission. It was taken down within a few hours and promptly disavowed by AOL as an "unauthorized freelance project." However, Pandora's box had already been opened, and thousands of people had already downloaded the software. Soon after its release, other programmers had reverse engineered the software and began disseminating the Gnutella source code as an open-source project. The


90. Varanini, supra note 28.


92. "An open standard describes a programming standard in which everyone that participates agrees to discuss and make any changes publicly. In other words,
Gnutella project has continued through the work of several groups, and nearly all of them are casually linked, not-for-profit entities.\footnote{\textit{...}}

\textbf{B. Gnutella's Software Architecture}

Gnutella's software architecture is markedly different than that of Napster. As discussed above, Napster uses a centralized server architecture, where a user logs on to a server or group of Napster-owned servers, connecting that user to others. In contrast, Gnutella is a decentralized network, directly connecting users and eliminating the need for an intermediary server. A user connects directly with another user, who then connects them with other users, and so on—creating a virtually limitless web of users spreading throughout the Internet.\footnote{\textit{...}} If a user has linked to you, they have also linked to virtually everyone to whom you have linked, and vice versa.\footnote{\textit{...}}

\begin{itemize}
\item it is a programming standard over which no one company has proprietary control \footnote{\textit{...}}
\item Bristol Tech., Inc. v. Microsoft Corp, 114 F. Supp. 2d 59 (D. Conn. 2000) (stating that Linux is an example of an UNIX based “open source” operating system updated continuously and by world-wide public programmers). In contrast to most commercial software where the owner does not permit users to view or to modify the software code, the public is encouraged to modify, and improve upon, the program. Other open source software includes Apache Web servers. Janelle Brown, \textit{The Gnutella Paradox}, SALON.COM, (Sept 29, 2000) at http://www.salon.com/tech/feature/2000/09/29/gnutella_paradox/.
\item Nerd Herd, one of such entities, is headed by Gene Kan and two other programmers. When asked what would happen if the RIAA would pursue legal action against Nerd Herd, Kan replied, “I'd be curious to see them try .... I mean, you can't get blood from a turnip. They wouldn't stand a lot to gain except maybe a few beat-up cars.” Varanini, \textit{supra} note 28, at http://music.gamespot.com/features/nerdherd/page3.html.
\item In a new user's initial Gnutella session, she will enter the Internet location of an established user. That established user, in turn, connects all the users to whom she has previously connected. Akansha Atroley, \textit{Napster: Music to Most Ears}, COMPUTERS TODAY, Aug. 15, 2000, at 80, \textit{available at} http://www.india-today.com/ctoday/20000801/trends.html. The query will continue to expand until a “horizon” of thousands of users is created. Chris Sherman, \textit{Napster: Copyright Killer or Distribution Hero?}, ONLINE, Nov. 1, 2000, at 16, \textit{available at} 2000 WL 1039749.
\item See Appendix Diagram B., adapted from an image at http://gnutella.wego.com/. (1) The Requesting User connects with her Initial Contact, and (2) that Initial Contact connects the Requesting User with other users. If the other users have a file that the Requesting User would like, (3) the file is transferred back through the Initial Contact, and (4) relayed back to the Requesting User.
\end{itemize}
Like Napster, the information contained in a Gnutella network is limited to the information that Gnutella users allow others to view on their machines while they are online. Unlike Napster, however, searches are not limited to MP3 or Windows Media files. A Gnutella user is able to search for any type of file, including word processing documents, movies, and other software. This capability, compounded by the increasing availability of high bandwidth connections, has already given the movie industry the same headaches that have been plaguing the music industry the past several years.

C. Legal Implications

Though the legality of “sharing” copyrighted works through Gnutella is as questionable as it is with Napster, Gnutella’s system architecture creates jurisdictional complications and other barriers to legally enforcing any judicial decisions that an aggrieved copyright owner might obtain. There are several reasons that Gnutella is more troublesome to copyright holders, including the nature of open-source software, and the lack of centralized servers.

Unlike Napster, Gnutella is open-source software that is not officially owned by any single company or entity. Rather, it is an application that is freely distributed and may be modified by any

97. This is in contrast to Freenet, discussed infra Section V, where files are distributed to users throughout the system, allowing other users to access the files even after the posting user logs off.


In June, online movie company SightSound.com agreed to place twelve films on the Gnutella network, which reportedly caused Mirimax, its partner company, to announce, “[w]e retain the right to immediately remove our films should we find their security is compromised.” Joseph Gallivan, Coming to a PC Near You, N.Y. POST, June 16, 2000, at 36, available at http://208.248.87.252/06162000/6193.htm; 2000 WL 22917248. SightSound has said that it would utilize encryption to protect its content. John Markoff, Disputed Software to be Used for Online Film Distribution, N.Y. TIMES, June 13, 2000, at C16, available at http://www.nytimes.com/library/tech/00/06/biztech/articles/14movie.html.

interested party. Several different versions of the software have become available since the original code was released, and hundreds of people have contributed to different permutations of the application. Furthermore, some aspects of Gnutella may eventually become an Internet standard, much like HTML, that may eventually spread throughout the Internet. Corporations have already begun to make the transition to peer-to-peer systems for their business-to-business ("B2B") transactions, making them more efficient, expedient, and secure than the current centralized exchange structure.

Since Gnutella is merely an application that is maintained by many loose-knit, non-profit entities, there is no single corporation or entity for a plaintiff to sue or for a court to shut down. Though an employee of America Online, Justin Frankel, initially created Gnutella, the source code has undergone several transformations since its release; it is arguably a much different program now than it was at its conception. America Online has been implicated for its role in the creation of Gnutella, but it could be difficult to hold the company liable for its existence, since it did not officially condone the project, it promptly removed the original program.
from its website, and it disavowed Gnutella soon after its creation.\textsuperscript{107} Even more, there are dozens of modified versions of Gnutella available,\textsuperscript{108} so it would be difficult to hold AOL liable for an application that looks very different than the version originally posted by AOL employee Justin Frankel.

Gnutella, unlike Napster, does not require any central servers to carry out its business, and is not a centralized target for plaintiffs to sue. Traditionally, copyright holders have been able to sue questionably infringing sites because the companies are identifiable, have a physical presence in a jurisdiction, and can be found on a machine in a specific geographic location.\textsuperscript{109} Such cases have included, among others, Napster,\textsuperscript{110} MP3.com,\textsuperscript{111} and MP3 Board.com.\textsuperscript{112} Those considering legal action against Gnutella, however, would not have the luxury of an easy target to sue, since the infringers and their computers may be located around the world and could number in the millions.\textsuperscript{113} Since there is no one company behind Gnutella, but it is only a loose-knit group of individuals who often participate in non-commercial file exchanges, copyright holders are left without any significant coffers to sue and some nearly insurmountable jurisdictional hurdles to overcome. Furthermore, any attempt by entertainment industry copyright holders would likely be a legal and public relations nightmare. The minimal damages that could be recovered from infringing users would not justify the cost and time involved in attempting to assert juris-

\begin{flushright}
107. Eunjung Cha, \textit{supra} note 87; Vogelstein \textit{supra} note 88.
\end{flushright}
diction against millions of individuals in a myriad of jurisdictions.  

V. FREENET

A. Background

Perhaps the most daunting of the current peer-to-peer systems is Freenet, developed by United Kingdom programmer Ian Clarke. Like Gnutella, it is decentralized, eliminating the need for central servers to direct users to other files on the network. What makes Freenet more threatening than its P2P cousins is its devotion to keep the source of the information passing through its system absolutely anonymous. Clarke views himself as a free-speech visionary with the mission of ridding the world of the concept of intellectual property.

In addition to decrying the idea of owning ideas, Clarke advocates Freenet as a tool to propagate free speech in political regimes rife with censorship, such as China and Saudi Arabia. Though Freenet proponents may periodically assert this legitimate use,
their marketing campaign is more focused upon Freenet's proposed elimination of intellectual property laws.\footnote{120}

Perhaps ironically, even though Clarke has been proselytizing the impending demise of intellectual property,\footnote{121} he has co-founded a company named Uprizer, which purports the ability to directly compensate artists for their works.\footnote{122} The precise manner in which the company will generate revenue remains a closely held secret.\footnote{123} Clarke has indicated, however, that his system’s idea draws upon author Stephen King’s success of offering installments on the honor system and threatening to stop the installments if too few users pay.\footnote{124} Applied to music, Clarke argues that artists may effectively cut out the recording industry middlemen.\footnote{125} Uprizer will join several other sites that are attempting to create a business model out of unlimited music distribution.\footnote{126}

\begin{itemize}
  \item[120] Interviews with Clarke have focused primarily on the revolutionary effect that Freenet will have on intellectual property, terrorist activities, and other criminal behavior. \textit{E.g.}, Schenker, \textit{supra} note 115, at 46, available at \url{http://www.time.com/time/magazine/articles/0,3266,47705,00.html}.
  \item[121] Clarke contends that “[t]he idea that you can treat information like you might treat real estate or gold is something that may have been possible to enforce in the past, but now with modern communication technology and particularly with systems like Freenet, that's just not a reality anymore.” Jan Hopkins, \textit{Freenet Founder}, CNNFN: STREET SWEEP, May 10, 2000, available at 2000 WL 4562603.
  \item[122] Clarke joined with Rob Kramer to form Uprizer, a company that hopes help artists profit from the distribution of music. Fridman, \textit{supra} note 118. Clarke argues that the record companies’ role of distribution has become obsolete with the advent of the Internet, and that recording artists are better off without copyright protection. \textit{Id}.
  \item[123] \textit{Id}.
  \item[124] King was initially successful with an honor system where users paid $1 for each unencrypted installment of “The Plant,” but as the novel progressed, fewer users had been paying the fee during download. Matthew Rose, \textit{E-Business: E-Books Have a Big Future, but It’s Unlikely to Come Anytime Soon}, WALL ST. J., Oct. 2, 2000, at B1, available at 2000 WL-WSJ 26611636. King abandoned the project, stating that too few users were upholding their end of the bargain. M.J. Rose, \textit{Stephen King’s ‘Plant’ Uprooted} (Nov. 28, 2000), at \url{http://www.wired.com/news/culture/0,1284,40356,00.html}.
  \item[126] Flycode (formerly known as AppleSoup) also intends to build a system that will compensate copyright owners for their material, though how they will do so is still a secret. Thor Olavsrud, \textit{AppleSoup: Revolutionizing the Napster Revolution?}, INTERNETNEWS.COM, (July 17, 2000), at \url{http://www.internetnews.com/bus-news/article/0,3,416531,00.html}. Mojonation.com is similar to Gnutella, but rewards those who upload a song with digital currency called “Mojo.” Damien Cave, \textit{The Mojo Solution: Forget Napster and Gnutella. Jim McCoy’s Mojo Nation is the Coolest File- Trading Service on the Net}, SALON.COM (Oct. 9, 2000), at \url{http://www.salon.com/}.
\end{itemize}
B. System Architecture

Like Gnutella, Freenet is a peer-to-peer, decentralized system. Each user's computer is labeled a "node," which stores and retrieves encrypted files that can be opened by text strings called "keys." The nodes pass the keys back and forth in an attempt to find the encrypted file that the key will unlock. Each node knows only its immediate neighbors, and it is extremely difficult to tell whether your requesting neighbor originated the search or simply passed along another user's request. When a file is found, it is stored on the both the requesting user's node and another user's node along the request stream. The encrypted file remains on...


129. Id.

130. Id.

131. Id. Under this system, if a copyright owner would want to search for infringements upon her intellectual property, the mere search would serve to...
both machines for a finite period of time, phasing out files not regularly searched for and keeping alive more popular files.\textsuperscript{132}

C. Legal Implications

Of the three file distribution systems evaluated by this article, Freenet presents the most difficult legal challenges, both in regard to enforcement of the law and to methods of prosecution. Clarke had five goals when designing Freenet, and each of them presents a distinct legal challenge that inhibits the enforcement of copyright. Clarke hopes to provide (1) anonymity for both sources and consumers of information, (2) deniability for those who store information, (3) resistance to attempts by third parties to prevent or limit access to information, (4) efficient dynamic storage and routing of information, and (5) decentralization of all network functions.\textsuperscript{133} If Freenet is successful in any of these areas, it will become a formidable challenge to those trying to stem the tide of copyright infringement via the Internet.

1. Anonymity For Producers And Consumers

Arguably, Freenet's most innovative attribute is its effective concealment of the source of information on the system. Napster's architecture makes it relatively easy to identify its users and the substance of their file sharing.\textsuperscript{134} Gnutella makes determining user identity more difficult, though still possible.\textsuperscript{135} Freenet, however, makes it nearly impossible to find the source of any information contained on its network since each user (or "node") only knows the requests of its immediate neighbor without having a larger knowledge of the entire network.\textsuperscript{136} Thus, it would be very difficult to propagate the file throughout the system, defeating her purpose. \textit{Id.}

\begin{itemize}
  \item \textsuperscript{132} \textit{Id.}
  \item \textsuperscript{133} \textit{Id.}
  \item \textsuperscript{134} Metallica, in preparation for its lawsuit against Napster, hired Internet firm NetPD to determine which users were trading Metallica files, and that firm presented to Napster a list of more than 300,000 usernames of individual trading such files. \textit{Napster Users Offering Pirated Metallica Songs Identified by Lawyers}, \textit{Wall St. J.}, May 3, 2000, available at 2000 WL-WSJ 3027885. \textit{See also} Mann, \textit{supra} note 79.
  \item \textsuperscript{135} With Gnutella, it would theoretically be possible to determine the origin of a file by tracing Internet Protocol (IP) addresses through the links of users who have passed on that information. Gnutella: View Support Pages, \textit{What is Gnutella}, http://gnutella.wego.com/ (last visited Jan. 10, 2001).
  \item \textsuperscript{136} Clarke, \textit{supra} note 128.
\end{itemize}
for a law enforcement authority to trace the source of the file more than one or two links up the chain.\(^{137}\) This leaves copyright owners with a very difficult question: How can one prosecute a distributor of copyrighted information if one cannot even determine the identity or the physical location of the distributor?

2. Deniability For Users Who Store Information

One of Clarke’s intentions in designing Freenet was to relieve node owners of culpability for any information stored on their machines. To this end, he made certain that Freenet users could not easily determine the nature or content of the files that Freenet has stored on their systems. For example, a node along the chain that passes on information to a requesting node also keeps a copy of that information for future requests.\(^{138}\) Freenet encrypts all these files, and it does not give a key to view the file’s contents to these storage nodes.\(^{139}\) Though it is mathematically possible to determine the contents of the information one has on one’s node, it would be highly impractical since it would require a complicated dictionary de-encryption program to decode the key.\(^{140}\)

Thus, it would difficult or impossible for law enforcement authorities to determine whether a user has illegal files on her hard drive. Not only is it difficult to determine who is using the system, even if the user is found, it is nearly impossible to determine whether she possesses infringing files. Moreover, even if a user wanted to find out if she was storing illegal or copyright-infringing files, it would be nearly impossible for her to do so.\(^{141}\)

Being able to deny any knowledge of the contents of one’s machine might provide Freenet users with at least two defenses under

\(^{137}\) Id.

\(^{138}\) Id.

\(^{139}\) Id.

\(^{140}\) Id.

\(^{141}\) Again, though decryption of the file would be mathematically possible, it would be unlikely to be enforced as a practical matter, considering the complexity of its implementation. Sean Flinn, The Digital Hive: Freenet Developer Ian Clarke Explains how His Creation will Revolutionize the Internet. ZDNET MUSIC, at http://music.gamespot.com/radiospy/articles/ianclarke_4.html (last visited Jan. 4, 2001). Clarke says, “It is not mathematically impossible to identify people on Freenet. What we would say—and what we hope and what nobody has yet been able to dispute—is that it is, for all practical purposes, impossible to identify somebody on Freenet.” Id.
the Digital Millennium Copyright Act ("DMCA"). In the DMCA, service providers are provided a "safe harbor" under which they are not held responsible for transitory digital network communications and system caching.

Freenet users would likely fall under the "transitory digital network communications" category since the transmission was initiated by someone other than the user, the transmission was automated, the user does not select the recipients, and the material is not modified during the transmission. There may be a question as to whether section 512(a)(4), which requires that the information not be "ordinarily accessible to anyone other than anticipated recipients," is satisfied since others would subsequently be able to access the material.

An equally strong argument is that the mirroring of the information on a user's machine would constitute "system caching" under section 512(b). Freenet users also fall under this category since the users themselves are not accessing the information, but its location on their machines merely serves a caching function for other users. One question is whether Freenet users adhere to Section 512(b)(2)(B)'s requirement that a user "complies with rules concerning the refreshing, reloading, or other updating of the material when specified by the person making the material available online in accordance with a generally accepted industry standard data communications protocol." This may, however, be mitigated since such a protocol does not yet exist.

Like service providers, it is unlikely that Freenet users would be required to constantly police their systems for infringing content. Even more than service providers, Freenet users have the additionally high burden of decoding encryption to even determine whether the information on their system infringes upon a copyright.

143. Id. § 512(a).
144. Id. § 512(b).
145. Id. § 512(a)(1)–(5).
146. Id. § 512(a)(4).
147. Netword, LLC v. Centraal Corp., No. 98-1023-A, 1999 U.S. Dist. LEXIS 1957, at *7 n.5 (E.D. Va. Jan. 12, 1999) (defining caching as "when a computer stores information in its memory, and at the direction of a software command, searches or polls that information to find the desired result").
149. Telephone interview with Michael McGuire, Associate Counsel, GMAC-RFC (Dec. 1, 2000).
Since it is very difficult for users to determine the nature of the information stored on their systems, how can they be held responsible for its content and potential infringement?

3. Resistance To Third-Party Attempts To Deny Access

Freenet has a built-in "immune system" that propagates a file each time it is requested, making a copy of the file on both the requester's node and on another unnamed user's node. For example, if User A requests File A from User B, a copy of File A is untraceably copied to User X's node. This transferring of files turns the enforcement of copyright into a game of whack the mole. Even if an adversarial user shuts down the known nodes carrying an objectionable file, the file has likely been copied to other unknown nodes that remain viable to disseminate the file.

This resistance also makes it difficult for copyright holders to even search the system to find out whether their content is being shared, much less force the Freenet users to cease and desist. For example, even if Metallica underwent a similar search for its material on Freenet as it did on Napster, it would defeat its purpose because Metallica's own searches would further the propagation of the files throughout the system.

4. Efficient Storage And Routing

In addition to its apparent legal and technological impenetrability, Freenet also employs advanced techniques to ensure that information in its system is passed along efficiently. As a Freenet

---

150. CLARKE, supra note 128.
151. See Appendix Diagram C, created by the author.
152. CLARKE, supra note 128. This system also avoids the dilemma of server crashes when too many users try to access information from one website. Id. In Freenet's system, the information has already been automatically duplicated to "mirror" nodes, alleviating network congestion and spreading the information to other unknown sources. The Freenet Project, Re-Wiring the Internet, at http://freenet.sourceforge.net/index.php?page=features#nohost (last visited Jan. 4, 2000).
153. Charles C. Mann & Roger Parloff, Napster Playing Dumb, Experts Say: Programmers Say the Company Could Easily Block Most of the Infringing Files From Its Directory, THESTANDARD.COM (Oct. 18, 2000) at http://www.thestandard.com/article/display/0,1151,19487-0,00.html (stating that Metallica and Dr. Dre hired Internet firm NetPD to determine which users were sharing the band's files).
node passes more and more files on to other nodes, it continuously remembers the system's configuration and transfers the files in a more efficient manner.\textsuperscript{155} Thus, if a certain document or file is popular in a specific geographic area, Freenet duplicates the data to the area in which it is in greatest demand.\textsuperscript{156} Currently, if a file on an Asian server is popular in America, the file remains on the Asian server, resulting in relatively slow file transmissions. If the file were made available on the Internet under Freenet's system, the popular file would duplicate itself on American nodes, thus decreasing the amount of time required to access the file.\textsuperscript{157}

Freenet's method of distribution builds upon the methods of Napster and Gnutella. Napster slows information requests by requiring the information to go through a Napster server before it is retrieved from the source computer.\textsuperscript{158} Gnutella, in contrast to Napster, is decentralized, but it is not as well suited for large-scale implementation.\textsuperscript{159} Some have expressed concern that Gnutella has an inherent flaw that prevents it from working effectively when its user base becomes too large.\textsuperscript{160} Freenet's proponents argue that Freenet does not have this design flaw and that Freenet's design is more scalable and efficient than its peer-to-peer cousins.\textsuperscript{161}

5. Decentralization Of Network Functions

Like in Gnutella, each Freenet user, or "node," connects with other nodes directly, using the other nodes as intermediaries.\textsuperscript{162} Like Gnutella, Freenet's decentralization makes it difficult or prac-
tically impossible to shut down because an enforcement authority would have to take control of every node on the system to bring about its demise. In an increasingly global Internet, it would be extremely difficult to bring this about, especially if some nodes were located in countries not friendly with the United States.

Freenet has a particularly problematic attribute: once made publicly available, it is difficult or impossible to take offline. Clarke has repeatedly emphasized the integrity of the system against any attempts to shut it down and has said that even if he wanted to, he would not be able to destroy his creation. Like its counterpart Gnutella, without a centralized server to confiscate and without a physical presence to take offline, Freenet is merely a piece of software that is used on the Internet. In addition, since it is nearly impossible to determine who is using the system, enforcing a ban of its use would be a nearly impossible task.

VI. SOLUTIONS FOR PEER-TO-PEER NETWORKS

A. Legislative Remedies

Congressional action to respond to the legal dilemmas created by technological innovations has a long history. While such remedies often resolve the problems present at the time of legislation, it is difficult to create a law that is broad enough to cover future innovations in technology, yet narrow enough to remain effective in its purpose. An example of legislation addressing a specific technology is the Audio Home Recording Act of 1992, which Congress passed in response to concerns about the potential for abuse using digital audio tapes ("DATs"). Although DATs

164. Id. Clarke has said, "If someone put a gun to my head and said, 'Shut this down,' I would be unable to do so." Id.
165. See supra text and accompanying notes 100-104.
169. See generally Gary S. Lutzker, DAT's All Folks: Cahn v. Sony and the Audio
never came into common use, the law was stretched out of its skin in an attempt to apply it to newer technologies such as the Diamond Rio MP3 player.\footnote{160}

Congress has examined the use of Napster and similar technologies in legislative hearings,\footnote{171} but legislators have chosen not to take action on the issues for the time being.\footnote{172} In May 2000, the Progressive Policy Institute ("PPI") recommended that Congress amend the DMCA to require organizations such as Napster to make their users more accountable for their actions.\footnote{173} The paper's dated recommendation unwittingly demonstrates the weakness in attempting to legislate remedies to today's technology by narrowly focusing on "service providers" like Napster.\footnote{174} The proposed change would likely not apply to Gnutella and Freenet, since these technologies would not likely be considered "service providers" under the language of the PPI recommendation.

Any similar legislation attempting to thwart Napster would not be likely to affect the burgeoning threat of decentralized systems such as Gnutella and Freenet.\footnote{175} Even if the legislation were drafted broadly enough to cover these latter technologies, it would likely be

\begin{quote}
\end{quote}


\footnote{171. Sean Silverthorne, Mr. Napster Goes to Washington, ZDNET NEWS (July 11, 2000), at http://www.zdnet.com/zdnn/stories/news/0,4586,2601519,00.html.}

\footnote{172. At a Senate Judiciary Committee hearing into whether lawmakers should intervene to control Napster, Sen. Patrick Leahy, D-VT stated that "[i]f you write a song ... you ought to be rewarded for that. At the same time let's not strangle the baby in the crib. Let's make it work." Reuters, Napster Users Mount E-Mail Campaign, ZDNET.COM (July 18, 2000), at http://www.zdnet.com/zdnn/stories/news/0,4586,2604615,00.html.}


\footnote{174. Ham & Atkinson, supra note 173.}

\footnote{175. Representative Howard Berman, Ranking Democrat on the House subcommittee on courts and intellectual property, looks favorably upon Congressional inaction, considering the development of Gnutella and similar technologies. Brad King, Legislating Property of the Mind, WIRED NEWS (Oct. 4, 2000) at http://www.wired.com/news/politics/0,1283,39110,00.html.}
too restrictive—and would constrain technological advances. The swift entrance of these technologies into the mainstream underlines the wisdom in waiting to legislate the issue. In addition, public sentiment seems to favor the sharing of music over the Internet—regardless of whether the information is copyrighted.

This finding indicates that a potential jury might not rule against a defendant system. With a large percentage of its constituents believing that copyrighted material should be traded without threat of legal recompense, Congress might have further reason to delay any action on the issue. Rather, Congress would be wise to allow the courts, technology, and the marketplace to determine the current law's applicability to copyright.

B. Technological Remedies

Technological methods may be the best present hope for combating copyright infringement, and several methods have been proposed to remedy the dilemma created by digital distribution methods. Though the proposals suggested are most often applied to audio files, the concepts are easily applied to all copyrightable material, including text and movies. Encryption and watermarks have been viewed as the best line of defense against music piracy. The difference between the two technologies is as follows: to view an encrypted file, a user must break the encryption, which is usually an algorithm. A watermark, on the other hand, is a code that is placed on top of the file, requiring that the file be used in conjunction with a compatible secure player or viewer before it is used.

176. There are several arguments opposing copyright legislation in light of rapid technological change. E.g., supra notes 2, 166, and 167.
177. A National Law Journal study done by DecisionQuest found that 41.5 percent of 1,000 potential jurors believe that copyrighted music should be freely traded for personal use. Dick Kelsey, Jury Pool Survey - Napster’s Chances Good, NEWSBYTES, Oct. 10, 2000, at http://www.newsbytes.com/pubNews/00/156450.html.
178. Id.
180. Supra Section VI(B)(1).
181. Supra Section VI(B)(2).
1. Encryption

One solution to the dilemma created by digital distribution is to encrypt the files so a user could only open them with a specific key, signifying that he is authorized to read or use the file. If copyright owners employ this method, consumers would be required to purchase the copyrighted material and would not be able to freely duplicating the content.

The strength of encryption as a means to stem the tide of copyright infringement is that it should work regardless of the distribution system. Whether the file is transferred via Napster, Gnutella, Freenet, or another similar system, an effective encryption scheme would prevent unauthorized parties from using the file.

The problem with encryption is that clever individuals often break the encryption scheme soon after it is released. After the encryption is broken, the method for cracking the code can be easily disseminated through the Internet. A recent example of the distribution of encryption workarounds can be found in the facts of Universal City Studios, Inc. v. Reimerdes, which dealt with the hacking of Digital Versatile Disc ("DVD") encryption technologies. In Reimerdes, The CSS technology touted by the industry to be a nearly unbreakable code was thwarted by a 15-year-old Norwegian boy who wanted to play DVDs on his Linux system. The movie studios sued 2600 Magazine because they originally posted—and later

---

182. E.g., Reimerdes, infra note 184. The SDMI coalition has challenged hackers to try to break their encryption in an attempt to strengthen the scheme's security. However, their offer of $10,000 to a hacker who successfully breaks the encryption has been met with a lukewarm response from the hacker community. Some speculate that the hacker community did not want to do the record companies' "dirty work" by strengthening their code. Sam Costello, Hackers reject $10,000 offer to break code, CNN.COM (Sept. 18, 2000), at http://www.cnn.com/2000/TECH/computing/09/18/picky.hackers.idg/index.html.

183. Some experts have resigned themselves to this reality, and have focused their efforts on two types of people: hackers, and common users. Though encryption may not deter the first group, companies can try to ensure that the decryption technology does not fall into the hands of the second group. Charles C. Mann, The Heavenly Jukebox: Efforts to Obtain Control Access to Sound Recordings from the Internet, ATLANTIC MONTHLY, Sept. 1, 2000, at 39, available at http://www.theatlantic.com/issues/2000/09/mann.htm, also at http://www.theatlantic.com/issues/2000/09/mann2.htm.

185. Id.
186. Id. at 311.
linked to—other sites that posted DeCSS, a method to de-encrypt DVD’s CSS technology.\textsuperscript{187} Encryption was not found to be a successful deterrent in its prior use in other software technology.\textsuperscript{189} In the 1980s, software creators used encryption techniques to deter hackers from engaging in piracy.\textsuperscript{190} However, the practice eventually fell out of favor because of the frustration that it caused mainstream consumers.\textsuperscript{191} The entertainment industry may see a similar consumer backlash in regard to encryption. Consumers are currently reluctant to adopt secure formats such as Windows Media and Liquid Audio when the unencumbered MP3 format is so widely available.\textsuperscript{192}

A more promising encryption technique may come from three Brown University mathematicians who have recently patented an encryption system that would require a separate encrypted key for each small portion of a file.\textsuperscript{193} One could encrypt music files, for example, to require a separate key for each second of recorded music.\textsuperscript{194} Thus, hackers would have to break an encryption scheme for each second of a music file, a much more arduous task.\textsuperscript{195} Though this method sounds promising, as with other encryption technology, other bright individuals are likely to be waiting in the wings to break this encryption method.

Judge Ferguson observed this difficulty with encryption during the trial phase of \textit{Universal Studios, Inc. v. Sony Corp. of America}:\textsuperscript{196} “[A]s sure as you or I are sitting in this courtroom today, some bright young entrepreneur ... is going to come up with a device to

\begin{itemize}
\item \textsuperscript{187} CSS stands for “Content Scramble System.” \textit{Id.} at 308.
\item \textsuperscript{188} In its final ruling, the trial court found that that 2600 may not link to the code, and that such linking is in violation of the Digital Millennium Copyright Act (“DMCA”) 17 U.S.C.A. § 1201(a)(2) (1998). \textit{Id.} at 325.
\item \textsuperscript{190} Barak D. Jolish, \textit{Scuttling the Music Pirate: Protecting Recordings in the Age of the Internet}, 17 SPG ENT. & SPORTS L. 9, 11 (1999).
\item \textsuperscript{191} Encryption on software created problems with installation and moving the software from one computer to another. \textit{Id.}
\item \textsuperscript{192} Malcolm MacLachlan, \textit{Critics Question Microsoft Audio Format}, TECHWEB News, Apr. 14, 1999, at 1.
\item \textsuperscript{193} U.S. Patent No. 6,081,597 (issued June 27, 2000).
\item \textsuperscript{195} \textit{Id.}
\item \textsuperscript{196} 480 F. Supp. 429 (C.D. Cal. 1979).
\end{itemize}
unjam the jam. And then we have a device to jam the unjamming of the jam and we all end up like jelly.” Indeed, encryption may not be the “holy grail of copyright” that some purport it to be.

2. **SDMI And Digital Watermarking**

Some have suggested that files be “watermarked”, or encoded, with its owner’s copyright information, making the files easy to locate, and enabling owners to control how their files are used. Such controls may include the number of times a file may be duplicated and the prohibited use of a non-encrypted file on “secure” devices.

One method of digital audio watermarking is being developed by the Secure Digital Music Initiative (SDMI), a consortium formed in December 1998. SDMI is not intended to be a technological standard, but it is rather a listing of requirements that a technology would need to be deemed “SDMI compliant.” There are nearly 180 companies in the initiative, and they include members of the recording industry, music hardware manufacturers, and other interested parties. The SDMI has been working to create a digital music standard since 1998, and it plans to implement this standard on portable music devices in two phases. Phase I was completed on June 28, 1999, and it was adopted by the five major recording companies in June 2000. Phase I allows portable devices to play


204. Jennifer Bales, *Industries Attempt to End Music Piracy with Watermarking*, U-
both secure files such as Windows Media files, and nonsecure files, such as MP3. Phase II, however, would require that a file be watermarked by SDMI to be played on an SDMI-compliant player. Thus, as it is currently composed, SDMI-compliant players eventually will not be able to play files in non-secure formats like MP3. Consumers, however, may be reluctant to adopt a format that is incompatible with MP3, the format with which they have become enamored for the past five years.

In September 2000, SDMI challenged hackers to break the encryption for five proposed technologies that were being considered for the final standard. SDMI offered $10,000 to anyone who could crack the watermark, in an attempt to strengthen the technology. Despite a hacker community boycott of the contest, SDMI still received 447 submissions and acknowledged that the integrity of two of the five technologies under consideration had been compromised. The success of the contest provides some hope that the balance between compensation of the copyright holders and the ease of use by consumers might be reached.

VII. CONCLUSION

Peer-to-peer distribution systems give millions of users the power to circulate their favorite song, book, or movie to millions of...


205. Phase I was designed to allow manufacturers to begin to comply with the standard before a final standard was complete. Stephen M. Kamarsky, Managing Copyright in Digital Marketplace System May Be Redefined by Music Distribution War, N.Y.L.J., Oct. 18, 1999, at S4.


207. Id.

208. Id.


210. Id.

211. The hacker community did not want to aid SDMI by providing cheap labor to create a more stringent encryption technology. Mike Musgrove, 'Watermarks' on Music Files Tested; Hackers Say They Can Break the Code, but Success is Subjective, WASH. POST, Nov. 2, 2000, at E01, available at 2000 WL 25425741. In the words of one hacker, "I won't do your dirty work for you ... Hackers should not, and will not, offer free consulting services to an organization that is using technical means to destroy the customary balance of interests of copyright holders and music listeners." Id.

212. Id.
others with very little to stop them—legally or technologically. However, there is a long history of new use technologies that initially seem to thwart copyright law, but are later used by copyright holders to their advantage. Arthur Miller gives us hope that our concerns about the Internet may be as unwarranted as concerns about the phonograph, television, and the photocopier.

Since the birth of copyright, every age has seen the emergence of a new medium of expression or technology that has led people to express the fear and concern that it defied the boundaries of existing doctrines or that the new candidate for protection was so strikingly different that it required separate legal treatment. In each instance, the copyright system has managed over time to incorporate the new medium of expression into the existing framework.213

Though technology nearly always moves more quickly than the law, we must find a manner in which we can compensate copyright holders without stifling technological advances. The Napster litigation gives us an indication of how peer-to-peer technologies will be treated by the courts, but Gnutella and Freenet demonstrate that technology is changing so rapidly that the legal issues brought by Napster will soon be obsolete. It remains a certainty that we, like those confronted with previous new use technologies, must devise a way to compensate copyright holders without stifling the growth of technology. If we are successful, Ian Clarke’s vision of a world devoid of copyright is unlikely to become a reality.

VIII. APPENDIX

Diagram A.

Diagram B.

Diagram C.

A cannot view X on network.

See supra note 96 for appendix sources.