The Digital Evolution:
Freenet and the Future of Copyright on the Internet

by Ryan Roemer

Introduction

Peer-to-peer ("P2P") technologies have created more criticism and praise than perhaps any other recent Internet technology. Working without the aid of a central server, P2P data sharing brings the Internet back to its roots, allowing users to connect directly with each other and exchange files. Unfortunately, bypassing these intermediary servers has left a legal system that assumes a central responsible party struggling to adjust.

In 1999, a college student named Shawn Fanning created a music file-sharing program called Napster. Napster almost immediately brought millions of users together, downloading and sharing an unprecedented amount of MP3[1] files, most of which were copyrighted musical works.[2] By December of 1999, as Napster's popularity gained, the record industry brought suit against Napster, Inc. for copyright infringement.[3] Although the recording industry eventually prevailed on their copyright claims and largely killed off most of Napster's user base, the damage had already been done. File-hungry users quickly flocked to the next generation of P2P technologies, which are adapting to new legal and technological hurdles at an amazing rate. The recording industry has since launched legal attacks on a variety of fronts, going after new P2P companies as well as individual users.[4]

This paper examines a developing technology named Freenet.[5] Freenet is a P2P architecture designed to be secure, efficient, and built to withstand virtually any legal or technological challenge. Although it is far too soon to predict Freenet's triumph or defeat, it is a worthwhile conceptual model to examine, because modern P2P systems are

[1] *See* Webopedia, MP3, *at* http://webopedia.internet.com/TERM/M/MP3.html (last visited Apr. 30, 2002).
[2] Mathias Strasser, *Beyond Napster: How the Law Might Respond to a Changing Internet Architecture*, 28 N. KY. L. REV. 660, 660-62 (2001).
[3] Andrew C. Frank, *The Copyright Crusade*, at 1, *available at* http://www.viant.com/pages2/downloads/innovation_copyright.pdf (last visited Apr. 30, 2002) [hereinafter Frank, *The Copyright Crusade*].
[4] *See* Adam Creed, *Judge Denies Betamax Defense For Morpheus*, Newsbytes (Mar. 5, 2002), *at* http://www.newsbytes.com/news/02/174951.html (last visited Apr. 30, 2002) [hereinafter, Creed, *Judge Denies Betamax Defense For Morpheus*]; Strasser, *supra* note 2, at 706.
[5] *See* The Freenet Project, *at* http://freenetproject.org/cgi-bin/twiki/view/Main/WhatIs (last visited Apr. 30, 2002).

already integrating many law-defying characteristics of Freenet and will continue to do so, even if the Freenet project never takes off.

The thesis of this paper is that the technology of P2P systems is stretching the applicability of modern copyright law to its limits. Content owners will possibly see the day that a technology like Freenet will render the current law ineffective against digital copyright infringement on the Internet. However, it is more likely that both P2P technology and copyright law will ultimately survive the current conflict intact, as they both adapt to legal and technological changes driven by worried content owners, digital libertarian programmers, and the file-hungry public.

Part I of this paper examines the technological nuances of Freenet and the trends in P2P projects to develop systems that withstand both legal and technological attack. Part II documents the ongoing battle between content owners and companies touting new, disruptive technologies that threaten copyrights, ranging from video cassettes to file-sharing computer programs. Part III examines how modern P2P technology tests the bounds of copyright law and content owners' available options to curtail full-fledged information anarchy on the Internet.

I. **Freenet and the Rapid Evolution of P2P Technology**

P2P technologies are spreading at an increasing rate, despite the persistent threat of legal action. Andrew Frank, Chief Technology Officer in Viant's Media and Entertainment practice, notes in *The Copyright Crusade*[6] that the "ironic effect" of the content industry's vigorous protection of copyrights in court was to create a "Darwinian force ... under which only the most legally and technologically resilient [file trading systems] survive."[7] P2P developers today focus on making copyright enforcement increasingly difficult, in addition to other technological goals.

Napster, Inc. believed it could escape secondary copyright liability by not directly transferring music files, but after losing in the Ninth Circuit in A&M Records v. Napster,

[6] *The Copyright Crusade* is a published study examining ways in which the content and media industries can address copyright implications of P2P technologies. *See* Abstract, *The Copyright Crusade*, *at* http://www.viant.com/pages2/pages/frame_thought_copyright.html (last visited Nov. 4, 2002).
[7] Frank, *supra* note 3, at 38.

Inc. ("*Napster*"), the service effectively shut down.[8] In response, "FastTrack" based P2P technologies[9] employ new distributed and encrypted "supernode"[10] servers to index file names and facilitate searching.[11] In addition to the technological robustness of distributed file indexing[12], it appears that the technology was also chosen to avoid the liability found in *Napster*. The content industry has wasted no time in pressing the issue of whether "FastTrack" companies can be liable under *Napster*, already filing suit against Grokster, Morpheus (StreamCast) and KaZaA.[13]

In contrast to the popular "FastTrack" technologies, many P2P developers are not focusing on "turning a buck," but rather on creating systems of file trading immune to both physical and legal attack. Perhaps the most advanced P2P technology in this regard is Freenet. Although the Freenet Project remains in the early stages of development, it has already created a secure P2P network that can withstand existing physical and legal attempts to shut down the network as a whole.

In July of 1999, Ian Clarke conceived of the idea for a secure, distributed file system during his studies of artificial intelligence and computer science at the University of Edinburgh, in Scotland.[14] The idea quickly progressed into an open source, volunteer-supported effort, known as the Freenet Project. Freenet was publicly released in March of 2000 and has been under frenetic development ever since.[15]

[8] A&M Records, Inc. v. Napster, Inc., 239 F.3d 1004, 1010-1011 (9th Cir. 2001) (holding Napster was not allowed to share copyrighted material specified by the plaintiffs), *aff'd in part and rev'd in part; temporary stay of preliminary injunction.*

[9] *See* Grokster, *Our Technology*, *at* http://www.grokster.com/technology.html (last visited Nov. 4, 2002).

[10] A supernode is a "peer" computer on a P2P network that also acts like a central server, maintaining a database of files and routing P2P searches from other peers. Many supernodes are used within a single P2P system, and any computer on a supernode-based system could potentially be a supernode.

[11] *See* Grokster, *Supernodes*, *at* http://www.grokster.com/helpfaq.html#SuperNodes (last visited Nov. 4, 2002).

[12] A collection of users' supernodes run the file indexing service, creating a situation where the purveyor of the P2P system has no control over the file index and the file index is mirrored on several uncontrolled supernodes, rather than a single server attributable to a specific company.

[13] *See* Electronic Frontier Foundation, *EFF "Intellectual Property - Peer-to-Peer (P2P) - MGM, Leiber, NMPA, et al. v. Grokster, MusicCity & Kazaa" Archive*, *at* http://www.eff.org/IP/P2P/MGM_v_Grokster (last visited Apr. 30, 2002).

[14] *See* Kevin Featherly, *Will Freenet Smash Copyright Law?*, Newsbytes (Mar. 202, 2002), *available at* http://www.computeruser.com/news/01/03/22/news11.htmlhttp://www.newsbytes.com/news/01/163395.html (last visited Dec. 4, 2002).

[15] *See id.*

A. **Freenet's Technology**

Freenet is not a "pure" P2P system (like Gnutella[16]), but is instead a distributed, caching file service.[17] The Freenet program includes a client that retrieves files from other Freenet user's computers ("nodes") and a server that relays requests and files for other Freenet clients on the network. The Freenet network operates without the aid of any central technology.[18] Each node of Freenet is autonomous and an "equal" on the system. Moreover, each node is aware only of nodes with which it can directly communicate. If a node disappears from the network, Freenet routes around this and the network continues unscathed.[19]

Unlike most P2P models, Freenet users who wish to share a file do not simply make a "shared" file available to other users and the network, like Napster or Gnutella do. Freenet users must "insert" the file into the Freenet.[20] Users create a "key" for the Freenet file such as "freenet:the_constitution.txt," and insert the file into their node. The file is then stored on one or more local Freenet nodes. As Freenet users request the new file, neighboring nodes make additional copies of the file, distributing it across the Freenet.[21] More popular files spread to more and more servers across the Internet. However, since Freenet servers have a limited storage capacity (determined by the node operator), less popular files get pushed out of servers and eventually drop off the Freenet altogether.[22]

[16] Gnutella operates by allowing a peer to search through other network peers until it finds a matching file, at which point the requesting and delivering peers directly connect to transfer the file. For an in-depth look at Gnutella, *see Knowbuddy's Gnutella FAQ*, *at* http://www.rixsoft.com/Knowbuddy/gnutellafaq.html (last visited Dec. 18, 2002).
[17] *See* The Freenet Project, *What is Freenet?*, *at* http://freenetproject.org/cgi-bin/twiki/view/Main/WhatIs (last visited Nov. 4, 2002).
[18] *See id.*
[19] *See* Karen Heyman, *Napster, Round 2: Genie 1, Bottle 0*, LA WEEKLY (May 26, 2000), *available at* http://www.laweekly.com/ink/00/27/cyber-heyman.shtml (last visited Nov 3, 2002) (quoting Ian Clarke: "I was fascinated by complex systems which consisted of individuals following simple rules, where no one individual was fundamental to the operation of the system. Consider a flock of birds in formation. If you were to shoot one bird, it wouldn't destroy the formation – because it doesn't rely on any one individual bird.").
[20] *See* The Freenet Project, *How to Publish Websites in Freenet*, *at* http://freenetproject.org/cgi-bin/twiki/view/Main/Publishing (last visited Nov. 4, 2002).
[21] *See* Heyman, *supra* note 19, available at http://www.laweekly.com/ink/00/27/cyber-heyman.shtml.
[22] *See* Ian Clarke et al., *Protecting Free Expression Online with Freenet*, IEEE INTERNET COMPUTING, 6(1) (Jan./-Feb. 2002), at 46, *available at* http://freenetproject.org/twiki/Main/Papers/ieee-final.pdf.

Thus, Freenet does not rely on specific nodes to serve requested files, but instead acts as a large "cache," bringing more popular files closer to the users who want them.

In *Napster*, the recording industry was able to document the widespread infringement of copyrighted songs because all of the communications between the central Napster server and clients were sent unencrypted across the network.[23] By contrast, Freenet encrypts all communications between nodes, so that third parties cannot monitor the content of file requests.[24] Additionally, files are inserted in encrypted form. Only after a file successfully reaches a requesting Freenet client's hard drive is the file decrypted into an identifiable form.[25]

Freenet also takes pains to protect and guarantee the anonymity of its users. In contrast to Napster, there is no central database of users, or even a concept of "users." Each node only knows the Internet Protocol ("IP") address of its neighbors.[26] When a file is retrieved or transmitted to a Freenet client, only the *last* node that contacts a monitoring node might be identified. However, there is no way of knowing whether that last node originated the file, or just passed on a "cached" copy from an earlier node. As files are requested and cached across the network, a node operator's server storage ("datastore") is used without the node operator's knowledge or control. A node operator cannot remove or determine what files are being served off of the node at any given point.[27]

[23] *See Napster*, *supra* note 8, at 1013-1014.
[24] *See* Clarke, *supra* note 22, at 45, *available at* http://freenetproject.org/twiki/Main/Papers/ieee-final.pdf.
[25] *See id.*
[26] Andy Oram, *Gnutella and Freenet Represent True Technological Innovation*, O'Reilly Network, *at* http://www.oreillynet.com/pub/a/network/2000/05/12/magazine/gnutella.html (May 12, 2000) (last visited Apr. 30, 2002); *see also* Brad King, *ISPs Face Down DMCA*, Wired News (Dec. 23, 2000) (describing Mediaenforcer, an online automated copyright enforcement tool that tracks down P2P infringers and contacts ISP's., and quoting President Travis Hill, who explains that while he "can't track everyone on Freenet, he claims [Mediaenforcer] can track the last person to come in contact with the information," because the next to last node in a Freenet search chain is visible to some observers.), (*available at* http://www.wired.com/news/print/0,1294,40816,00.html)
[27] *But see* E-Mail from Ian Clarke, to Ryan Roemer (Apr. 1, 2002, 11:42:44 AM PST) (indicating that if an observer had a list of "keys," they could match and identify data in a Freenet node datastore.) (on file with author).

B. **Freenet's Organizational Structure**

The Freenet Project aims to be robust organizationally, as well as technologically. Whereas Napster and others provide an obvious legal target of a central corporation to sue, Freenet is not the product of any specific company. The project currently consists of volunteer programmers, working on Freenet in their spare time.[28] Moreover, Freenet is an open source project, meaning that anyone who wishes to take the existing source code of the project and continue development on her own may do so unimpeded. Thus, Clarke contends, "Freenet is an open, democratic system which cannot be controlled by any one person, not even its creators."[29]

C. **Implications of Freenet**

The Freenet Project developers focused on four primary goals for their technology: to make it highly survivable, private, secure and efficient.[30] Freenet is designed to make it almost impossible to "shut down Freenet without shutting down the Internet."[31] The redundant caching of information and distributed system provides a network with no dependencies on a central server, or any node in particular. Simulated tests have shown that the Freenet system "is surprisingly robust against quite large [network] failures," working efficiently even when 30 percent of the system nodes were randomly removed.[32]

Freenet protects the anonymity of users inserting files into the Freenet and other users requesting and retrieving those files (through encrypted transmissions). Moreover, the node that delivered a file is likely not the node that originated the file. Thus, Freenet makes all information of activities (sharing and receiving) within in its scope private

[28] *See* The Freenet Project, *supra* note 17, *at* http://freenetproject.org/cgi-bin/twiki/view/Main/WhatIs.
[29] *Id.*
[30] *Id.*
[31] Heyman, *supra* note 16 (quoting Ian Clarke).
[32] *See* Clarke, *supra* note 22, at 48. Although it is beyond the scope of this article, Freenet is quite resilient against attacks on its network or file content. *See* Ian Clarke et al., *Freenet: A Distributed Anonymous Information Storage and Retrieval System*, Workshop on Design Issues in Anonymity and Unobservability (2000) (detailing Freenet's resilience against eavesdropper attacks to compromise anonymity and attempts

from the many prying eyes of governments, copyright owners and other interested parties.[33] Clarke characterizes the system as "a near-perfect anarchy."[34]

Freenet was originally conceived as a more efficient way to distribute information, later lending itself to the political goals of creating a haven for free speech.[35] The technological nuances of Freenet that yield particularly troubling legal quagmires also contribute to the Freenet system's very effective distribution of data. By dynamically caching data, files are copied to relaying servers. Subsequent requests do not have to go quite so far to get the file, as it is now available from any of the relaying nodes, saving substantial amounts of bandwidth. Simulated tests and analysis of the current network suggests that the Freenet model will be able to handle an enormous level of traffic and activity.[36]

D. **Status of Freenet Today**

The Freenet Project has progressed rapidly from Clarke's original concept paper to a working software program and network. Downloads of the software have already topped 100,000, while it is estimated that a new 1,500 users download the software every day.[37]

Despite growing popularity, Clarke is quick to point out that Freenet is not the "next" Napster because "Napster is an application, but Freenet is a platform."[38] Freenet is an architecture, which, like the Internet itself, can be used by programs for not only file sharing, but practically any form of communication. Developers are actively working on a variety of applications to take advantage of the security and distributed power of the Freenet network. The Freenet Message Board ("FMB") allows messages to be freely

to disable the Freenet network as a whole, such as denial-of-service attacks), (*available at* http://freenetproject.org/cgi-bin/twiki/view/Main/ICSI.

[33] *Id.*

[34] *See* John Markoff, *The Concept of Copyright Fights for Internet Survival*, N.Y. TIMES, (May 10, 2000), *available at* http://www.nytimes.com/library/tech/00/05/biztech/articles/10digital.html.

[35] *See* Heyman, *supra* note 19 (stating Clark's "motivation in creating Freenet was not political, but, rather, technical").

[36] *See* Clarke, *IEEE*, *supra* note 22, at 47-48.

[37] *See* Sean Flinn, *The Digital Hive*, Choler Magazine, (July 28, 2000) (interview with Ian Clarke), *available at* http://www.choler.com/articles/ianclarke.shtml.

[38] Shannon Cochran, *Freenet Casts Wide*, Dr. Dobb's Journal, (Feb. 22, 2001), *available at*

exchanged over the Freenet.[39] Far more ambitious is the "Everything Over Freenet" Project, which aims to implement a variety of services, such as email, news, chat programs, and DNS[40], over the Freenet.[41]

Nonetheless, the file-swapping public and recording industry are most interested in how easily users can trade content files over the Freenet. In this regard, content owners can breathe easy. At the current time, Freenet is a limited tool for everyday users. Freenet is still quite difficult to install and the network is very slow.[42] Moreover, Freenet currently lacks "free text" searches.[43] A Freenet user has to know the exact file name "key" to retrieve a given file. Searching for the key "freenet:theconstitution.txt" will not match to "freenet:The Constitution.txt" or any other variant that is not the exact file key, character for character.

E. **P2P and File-Sharing Trends**

Riding this wave of popularity, P2P systems continue to develop and adapt to both technological and legal changes. New P2P systems are sprouting up all over the Internet.[44] Moreover, broadband technologies, which allow greater download speed and use of these systems, are also expanding rapidly in the home and business environments. Freenet may not be the secure P2P system that ultimately gains a wide public acceptance, but it certainly serves as a conceptual model for future secure P2P technologies.

The large audience of file sharers are just as adaptive as the technologies they use, easily shifting to new P2P systems that better serve their needs. At the same time as the Ninth Circuit effectively shut down Napster, MusicCity offered its new FastTrack-based

http://www.ddj.com/news/fullstory.cgi?id=3188 (last visited Oct. 30, 2002).

[39] *See* The Freenet Project, *Third Party Tools*, *at* http://freenetproject.org/cgi-bin/twiki/view/Main/Tools (last visited Oct. 30, 2002).

[40] *See* Webopedia, DNS, *at* http://webopedia.internet.com/TERM/D/DNS.html (last visited Oct. 30, 2002), ("Short for Domain Name System (or Service), an Internet service that translates domain names into IP addresses.").

[41] *See* Everything Over Freenet, *at* http://eof.sourceforge.net/ (last visited Oct. 30, 2002).

[42] *See* Cochran, *supra* note 38.

[43] Oram, *supra* note 26.

[44] *See e.g.,* OpenP2P.com, *at* http://openp2p.com (detailing recent developments in everything from open source P2P projects to enterprise business applications of P2P technologies to the law governing P2P projects)(last visited Nov. 2, 2002).

P2P client, Morpheus.[45] Morpheus was an instant success and has now surpassed even Napster's load of simultaneous users.[46] Andrew Frank observed that Morpheus "illustrates how, despite user interface woes and a hostile legal climate, a new peer-to-peer service can still double its usage in the span of a month and emerge from nothing to become a hit."[47] The public has extremely low "switching costs," having no apparent problem abandoning their current P2P application for a new one, and is thus likely to migrate to the best P2P system, whether it respects copyrights or not.[48]

II. **The Current Digital Copyright Regime**

Copyright law has been the traditional sword the content industry wields against new technologies which are perceived as a threat.[49] The Internet may be the darling new technology of the day, but the present P2P situation is far from the first battle that the content industry has waged.[50] The tour of the modern confrontation between technology and copyright owners began in 1976, with Sony Corp. of Am. v. Universal City Studios, Inc. (hereinafter the "*Betamax*" case).[51]

A. **The *Betamax* Case**

Sony sold "*Betamax*" recording devices and tapes that allowed the public to record television programs.[52] Two moguls of the television content industry, Universal City Studios and Walt Disney Productions, quickly brought suit against Sony for

[45] Frank, *supra* note 3, at 24.
[46] *Id.* at 25.
[47] *Id.*
[48] *Id.*
[49] *See* Jessica Litman, DIGITAL COPYRIGHT 77-88 (Prometheus Books 2001). In her chapter entitled "Choosing Metaphors," Professor Jessica Litman outlines how copyright owners have been recasting the public's interests in copyrights as "loopholes," to gain more control over their rights. Litman also notes that technologies that threaten any financial interests have recently been a primary focus of attack of late, as the content industry attempts to define more and more (traditionally protected) conduct as "piracy."
[50] *See id.*, at 101-10 (detailing the content industry's skirmishes with player piano rolls and the incentives that copyright restrictions create on new technologies).
[51] Sony Corp. of Am. v. Universal City Studios, Inc., 464 U.S. 417 (1984).
[52] *Id.* at 422-23.

secondary copyright infringement.[53] Universal and Disney contended that Sony should be liable for the copyright infringement of consumers who utilized the Beta system, which made the simple copying possible.[54]

The Supreme Court decided *Betamax* in 1984. In a 5-4 decision, the Court held that Sony was not liable for secondary copyright infringement because Beta was an "article of commerce," which was "capable of substantial noninfringing uses."[55] The Court further reasoned that consumers who recorded television shows to play back at a later time ("time-shifting") were engaging in a legitimate "fair use", even if the copying was unauthorized by the copyright owners.[56] Although a narrow decision, *Betamax* had far-reaching legal consequences. The doctrine of "substantial noninfringing use" has now become the standard by which to judge potentially infringing technologies and products.

B. ***Napster***

In 1999, the popular success of Napster brought an almost immediate lawsuit against the file swapping service in A&M Records, Inc. v. Napster, Inc. (hereinafter "*<u>Napster</u>*").[57] The recording industry alleged that the vast majority of the MP3 files traded by the millions of Napster users were unauthorized copies.[58] Napster responded with several theories under which the activity that Napster supported was defensible. Both the district court and Ninth Circuit sided with the recording industry.[59]

Napster argued that actions of its users in swapping files were protected fair use under the theory that Napster users were engaged in "space-shifting" their music from CD's to computers, devices, etc. in the same way that Betamax users "time-shifted" television programs.[60] The Ninth Circuit concluded that the "shifting" defense was only available where a technology" did not also simultaneously involve distribution of the

[53] *Id*. at 420-22.
[54] *Id*. at 420.
[55] *Id*. at 442.
[56] *Id*. at 442-455.
[57] A&M Records, Inc. v. Napster, Inc., 239 F.3d 1004 (9th Cir. 2001).
[58] *Id*. at 1013, 1019, 1022.
[59] *Id*. at 1028-29.
[60] *Id*. at 1019.

copyrighted material to the general public. Time or space-shifting copyrighted material was only protected when essentially done for personal use."[61]

Napster was first charged with contributory copyright liability, because it had knowledge of, and materially contributed to its users' copyright infringement.[62] Napster argued that *Betamax's* "substantial noninfringing use" doctrine protected them from contributory copyright liability.[63] The Ninth Circuit considered Napster's possible noninfringing "capabilities," but concluded that the doctrine was unavailable to Napster because they had notice and actual knowledge of infringement.[64] The court also found that Napster materially contributed to copyright infringement by providing software and the central server.[65] Thus, the court sustained an injunction for plaintiffs on their contributory liability claim.[66]

Napster was also charged with vicarious copyright liability, because Napster "has the right and ability to supervise the infringing activity and also has a direct financial interest in such activities."[67] The Ninth Circuit found that Napster's business model depended on attracting a large user base to gain revenue. Thus, the pirated music available on Napster directly benefited the defendant.[68] The court then examined Napster's ability to supervise its users and found that it sufficiently could.[69] The court observed, "The ability to block infringers' access to a particular environment for any reason whatsoever is evidence of the right and ability to supervise."[70] The court held that Napster's police power "must be exercised to its fullest extent. Turning a blind eye to detectable acts of infringement for the sake of profit gives rise to liability."[71] Because Napster had not adequately supervised users and directly financially benefited from

[61] *Id.*
[62] *Id.* at 1020.
[63] *Id.*
[64] *Id.* at 1020-22.
[65] *Id.* at 1022.
[66] *Id.*
[67] *Id.* (citations omitted).
[68] *Id.* at 1023.
[69] *Id.* at 1023-24.
[70] *Id.* at 1023.
[71] *Id.*

copyright infringement, the Ninth Circuit concluded that an injunction was appropriate on vicarious liability grounds as well.[72]

C. **Grokster**

After Napster was saddled with the Ninth Circuit's injunction and the once thriving file-swapping service lost its luster, the public found KaZaA[73], Morpheus[74] and Grokster[75] (hereinafter "FastTrack" technologies), based on the proprietary "FastTrack" technology.[76] A FastTrack network relies on a collection of "supernodes" to provide listing and searching functions to users (like the old Napster central server).[77] Unlike Napster, actual users run supernodes, and not a FastTrack company.[78] The FastTrack companies claim that they have no knowledge of what goes on between the supernodes, as they do not directly control them and all supernode communications are encrypted.[79]

Following an increasingly standard approach to P2P technologies, the recording, music publishing and motion picture industries filed suit against the companies responsible for KaZaA, Morpheus, Grokster and FastTrack in 2001 (hereinafter the "*Grokster*" litigation).[80] Although the *Grokster* lawsuit is still in preliminary phases at the time this article was written, the filings and motions of both sides provide a good indication of the eventual legal showdown. The parties have filed various motions and responses. As of December, 2002, both sides have argued summary judgment motions in federal court, hoping to prevail before the case actually goes to trial.[81]

[72] *Id.* at 1024.
[73] *See* http://www.kazaa.com.
[74] *See* http://www.morpheous-os.com.
[75] *See* http://www.grokster.com.
[76] In February of 2002, StreamCast Networks switched the reliance of Morpheus from the FastTrack software, to the open source Gnutella network. *See* John Borland, *Morpheus looks to Gnutella for help*, News.com (Feb. 27, 2002), *at* http://news.com.com/2100-1023-846944.html.
[77] *See* Grokster, *Our Technology*, *at* http://www.grokster.com/technology.html (last visited May 8, 2002).
[78] *Id.*
[79] *Id.*
[80] Creed, *Judge Denies Betamax Defense For Morpheus.*, *supra* note 4.
[81] *See* John Borland, *File traders, studios spar in court*, News.com (Dec. 2, 2002), *at* http://news.com.com/2100-1023-975801.html (last visited Dec. 18, 2002).

The content industries claim that the *Grokster* defendants profit from users' copyright infringements like Napster, and are presently suing for both contributory[82] and vicarious copyright liability.[83] The plaintiffs allege that FastTrack defendants have actual knowledge of user infringement and that they actively encourage the public to trade unauthorized copyrighted works.[84] The plaintiffs further contend that the defendants control users' copyright infringements because they reserve rights to unilaterally terminate user accounts.[85] Finally, the plaintiffs argue that the defendants have derived financial benefit from the infringement of the content industries' copyrights.[86] Defendant StreamCast's[87] motion for partial summary judgment hints at the *Grokster* defendants' strongest arguments against secondary copyright liability under *Napster*: first, the defendants were running a network that was capable of "substantial non-infringing uses" protected under *Betamax*, and second, the defendants do not maintain a central database of available files like Napster.[88]

StreamCast initially noted that its Morpheus network has several non-infringing uses, leveraging the fact that Morpheus allows the exchange of any kind of document type (as opposed to only MP3's on Napster). One of Morpheus's non-infringing uses is Project Gutenberg's distribution of public domain "eBooks."[89] Another current use of the Morpheus network is the availability of government documents.[90] Third, copyright

[82] Plaintiffs' Class Action Complaint for Copyright Infringement at 23-24, Leiber v. Consumer Empowerment BV, No. 01-09923, (C.D. Cal. filed Nov. 19, 2001), *available at* http://www.eff.org/IP/P2P/MGM_v_Grokster/20011119_complaint.pdf [hereinafter NMPA, *Complaint*].

[83] *Id.* at 24-25.

[84] *Id.* at 19.

[85] *Id.* at ¶ 67.

[86] *Id.*

[87] Formerly known as MusicCity, StreamCast Networks offers the Morpheus P2P client.

[88] Defendant's Memorandum of Points and Authorities of Defendants StreamCast Networks, Inc. (Formerly Known As MusicCity.com, Inc.) And MusicCity Networks, Inc. in Support of Motion for Partial Summary Judgment at 2-3, Metro-Goldwyn-Mayer Studios, Inc. v. Grokster, Ltd., No. 01-08541 SVW (PJWx) (C.D. Cal. filed Jan. 22, 2002), *available at* http://www.eff.org/IP/P2P/MGM_v_Grokster/20020122_streamcast_memo_sum_judg.pdf [hereinafter StreamCast, *Motion for Partial Summary Judgment*].

[89] *Id.* at 11-12 (quoting Project Gutenberg CEO, M. Tally George) ("Project Gutenberg seeks to convert to digital form, and widely distribute over the Internet, many different types of documents from the King James Bible to Shakespeare to the CIA World Fact Book. The Morpheus software allows more de-centralized (and thus less expensive) distribution of Project Gutenberg's eBooks.").

[90] *Id.* at 12 (noting the timely availability of video files of President George W. Bush's address after the September 11, 2001, World Trade Center attacks).

owners utilize Morpheus to distribute authorized and protected media.[91] Finally, Morpheus allows the authorized exchange of demonstration, shareware[92] and freeware computer software.[93] Moreover, StreamCast concluded that if the Morpheus system could not utilize a *Betamax* defense ("staple article of commerce" defense), then liability would have to extend to most common internet technologies (like web servers, e-mail, FTP programs, etc.).[94] In opposition, the content industry contended that these "legitimate" uses are insubstantial in the face of widespread piracy and that most often such files cannot be found on the defendants' networks.[95]

StreamCast also argued that because it does not operate a central file-index server, it could escape liability under *Napster*.[96] Since FastTrack networks rely on user-controlled "supernodes" for file indexing, the *Grokster* defendants retain no control over the network or any supernodes.[97] Moreover, StreamCast observed, "If [StreamCast] ceased to operate, or if its servers became inoperative . . . the searching, indexing, transferring, downloading [and other] functions . . . would continue unaffected."[98] The content industry countered that the *Grokster* defendants retain control and knowledge of the content on their networks. Initially, the Morpheus program can recognize and determine similar files, which implies filters could be used to prohibit downloads of copyrighted works.[99] Moreover, StreamCast regularly updates the software[100], sends promotional and other information[101], and monitors its bulletin boards[102] from a central

[91] *Id.* at 12-14.
[92] *Id.* at 14-15.
[93] *Id.* at15.
[94] *Id.* at 24-25.
[95] Plaintiff's Memorandum of Points and Authorities in Opposition to Motion for Partial Summary Judgment of Defendants StreamCast Networks, Inc., (Formerly Known as MusicCity.com, Inc.) and MusicCity Networks, Inc. at 3, Metro-Goldwyn-Mayer Studios, Inc. v. Grokster, Ltd., No. 01-08541 SVW (PJWx) (C.D. Cal. filed Feb. 15, 2002), *available at* http://www.eff.org/IP/P2P/MGM_v_Grokster/20020215_riaa_mpaa_opp_memo.pdf [hereinafter MGM, *Opposition to Partial Summary Judgment*].
[96] *See* StreamCast, *Motion for Partial Summary Judgment, supra* note 89, at 6.
[97] *Id.* at 5.
[98] *Id.* at 7.
[99] MGM, *Opposition to Partial Summary Judgment, supra* note 96, at 6.
[100] *Id.* at 7.
[101] *Id.* at 8.
[102] *Id.* at 9.

location. Finally, the language of the Morpheus end user license proves that "Morpheus is an ongoing, interactive service that [StreamCast] can terminate at any time."[103]

StreamCast contends that for a product to avoid secondary copyright liability under *Betamax*, it "need merely be capable of substantial noninfringing uses."[104] StreamCast argues that "capability" was the crux of the Supreme Court's holding, and not the amount or degree of actual copyright infringement.[105] Thus, StreamCast concluded it would be protected because "Morpheus software is capable of present and future substantial noninfringing uses."[106] The content industry plaintiffs responded that these uses were not significant because the overwhelming majority of files traded on the FastTrack networks are illegal copies of copyrighted works.[107] Moreover, since the *Grokster* defendants have actual knowledge of infringement and the FastTrack system was designed solely to circumvent copyright liability, the defense is unavailable.[108]

Turning to the *Napster* decision, StreamCast contended that the Ninth Circuit only held Napster, Inc. liable for its conduct, and not its architecture.[109] Because StreamCast does not have knowledge of files indexed on supernodes and does not "'operate' the Morpheus user network," this architectural distinction precludes copyright liability under *Napster*.[110] The content industry responded that *Napster* precludes any *Betamax* defense because of actual knowledge and control.[111] The Central District of California denied StreamCast's motion and the case is set to go to full trial. Nonetheless, these arguments certainly provide a strong indication of the defining legal issues for the trial phase. Moreover, StreamCast's approach gives insight into the shifting legal landscape surrounding evolving file-sharing technologies. P2P projects, like Freenet, are mindful of the shaky legal ground on which they operate, and have adjusted to the *Napster* decision. The outcome of the *Grokster* litigation will likely further influence the design approaches of law-defying P2P technologies.

[103] *Id*. at 8.
[104] StreamCast, *Motion for Partial Summary Judgment, supra* note 89, at 17 (quoting *Betamax*, 464 U.S. at 442).
[105] *Id*. at 19-20.
[106] *Id*. at 20.
[107] MGM, *Opposition to Partial Summary Judgment, supra* note 96, at 12-13.
[108] StreamCast, *Motion for Partial Summary Judgment, supra* note 89, at 12.
[109] *Id*. at 22.
[110] *Id*. at 23.

III. **The Future of Copyright and Evolving P2P Technologies**

Freenet makes an interesting study as a technological solution to the legal problems of censorship on the Internet. Ian Clarke's goal of destroying copyright law, as it conflicts with free speech, is an equally tantalizing legal subject, given that legal systems tend to be inhospitable towards deliberate attempts to circumvent the law.

Several technical aspects of Freenet have perplexing legal implications. First, any attempt to monitor activity on the Freenet will be limited and difficult. Freenet's encryption and communication methods make observation of a node or the network impracticable. As a result, monitoring and documenting wide-scale copyright infringement, like in the *Napster* case, is presently impossible with a system like Freenet.[112] Second, Freenet's distributed "caching" system prevents data from being forcibly removed. If a court orders the takedown of material, a single node might be able to comply, but there is no way to filter or enforce the restriction on the network as a whole.[113] The caching system also makes it virtually impossible to identify the source of the original document.[114] The owner of a node serving up a file could be the original poster of the document, or the node could simply be one of thousands of nodes that unknowingly "cached" the document. Third, Freenet has no technical point of control. It was designed from its inception to be impossible to shut down, even by its own creators.[115] Freenet nodes can survive on a hostile system, even when other nodes are shut down or turned maliciously against the network.[116] Thus, legal or technological action against Freenet may prove fruitless against the system as a whole.

Additionally, it is worth considering that although copyright law may be effective at restraining P2P companies, it has done little or nothing to stop "direct" infringers - the

[111] MGM, *Opposition to Partial Summary Judgment, supra* note 96, at 14.
[112] Featherly, *supra* note 14.
[113] Moreover, since the only way a document disappears from the Freenet is by not being requested and getting pushed out of a node's datastore, verifying that a document is gone (by requesting it) would actually further propagate the document across Freenet.
[114] Frank, *supra* note 3, at 8.
[115] The Freenet Project, *supra* note 17 ("Freenet is an open, democratic system which cannot be controlled by any one person, not even its creators.").
[116] *See* Clarke, *supra* note 22, at 47-48.

millions of users trading files, with virtually no regard for copyright law.[117] Moreover, these users move seamlessly from one P2P system to the next, as demonstrated in the rapid rise of the FastTrack system from Napster's ashes. Thus, regardless of the specific technology (Morpheus, Freenet, etc.) shut down next, the core dilemma remains, as the public's insatiable thirst for file trading is met by new and evolving technologies.

A. **Enforcing Copyrights Against Individual Freenet Users**

In *Napster*, although the recording industry did not pursue legal action against individuals, it had no difficulty discovering evidence of Napster users' "direct" copyright infringement by monitoring the Napster network. Unfortunately, even this is wrought with technological, legal and practical difficulties on a system like Freenet. Freenet's encrypted storage and communications, and lack of central communication point, prevent any party from monitoring general activity on the network. Furthermore, Freenet traffic looks very similar to other services, hindering the determination of which computers are even *running* the Freenet, let alone what files they are sharing..[118]

The Freenet system also complicates the individual user liability model under *Napster*. Clearly Freenet users who illegally download copyrighted works are guilty of infringing reproduction, but what of the nodes that serve the content? In *Napster*, individual users chose to share files they had stored on their computers, presumably infringing copyrights in distribution. By contrast, Freenet node operators never know what content is actually cached on their nodes, and have a plausible argument that they had no part in any actual infringement.[119] Fred von Lohmann, an attorney with the Electronic Frontier Foundation, opines that Freenet's automated caching system, "minimize[s] the likelihood of direct infringement liability" for node operators, because it

[117] *See* Litman, *supra* note 49, at 168-69.

[118] Clarke, *supra* note 27 ("The traffic right now looks like random data, since it is encrypted from the outset. It also runs on a randomly selected TCP port. Lastly, a Freenet node will not reveal that it is a freenet node unless you prove that you know its public key - which makes port-scanning virtually impossible. All of this would make it very difficult for an ISP to scan for Freenet nodes, however by running a freenet node, one can passively collect the IP addresses of other nodes in the network. This would be of little use to an ISP looking for a specific IP address, since it is rather improbable that they would stumble across that node's IP address in a large Freenet network.").

[119] Moreover, any stored content is always subject to change, as new data pushes out the old.

was designed for efficiency reasons.[120] Moreover, the process by which a copyright owning plaintiff would actually prove individual infringement complicates the situation even more. Because Freenet replicates popular data, if a plaintiff requested and received a file from a neighbor node, it is very likely that the plaintiff's very request *actually placed* the file on the offending node![121] Thus, Freenet's caching system, where users and computers no longer control and own files, makes legal action against direct copyright infringers difficult.

In addition, even if individual liability were legally plausible, copyright owners could not go after the most wanton infringers. Traditionally, a P2P system (like Napster or Gnutella) is driven by small groups of users (the "big dogs"), who provide most of the files. While it is infeasible to sue *everyone* on a P2P network, going after the major suppliers of information is a somewhat effective legal strategy. [122] However, this tactic is completely ineffective for Freenet, because node operators do not control or know what is on their node. Someone else most likely inserted the original infringing file, and eventually got "cached" at some given user's node. On Freenet, node operators cannot be reliably identified and distinguished as saintly, copyright-obeying users versus willful, copyright pirates and distributors.

B. **Enforcing Copyrights Against Organizations Promoting Freenet**

Copyright owners usually forego legal action against individual infringers, concentrating instead on identifiable companies releasing the technologies. However, Freenet is difficult to target as an organization. Freenet itself is not "owned" by any one entity. The Freenet Project does not operate for profit, and relies almost entirely on the volunteer efforts of developers. Freenet is an open source project, allowing anyone to

[120] *See* Fred von Lohmann, Protecting Clients: Legal Impact of Filesharing Network Design, InfoAnarchy Post (Aug 10, 2001), *at* http://www.infoanarchy.org/story/2001/8/9/193714/7327
[121] *See* King, *supra* note 26 (stating one can only determine identity of next-to-last node in search chain).
[122] Litman, *supra* note 49, at 167 (stating the RIAA even went after "scores" of student websites hosted at universities).

take the source code and continue independent development.[123] Andrew Frank sums up the difficulty in initiating legal actions against such projects:

> Going after the creators of such services does little good: first, these systems are generally being developed using Open Source collaboration, so hundreds of anonymous developers worldwide may contribute to the final product; second, even if these alleged perpetrators could all be identified and prosecuted, they would not be able to stop the service once it was unleashed, as it would be running on the individual computers of its users.[124]

Professor Jessica Litman, in *Digital Copyright*, echoes this sentiment, noting, "As a comprehensive strategy, litigation works best against commercial actors."[125] Litman concludes that a litigation strategy will prove increasingly difficult for programs that offer no clear intermediary to sue, like The Freenet Project.[126]

Nonetheless, it is possible (some would say even likely) that Freenet developers could eventually become a legal target. However, traditional copyright law does not lend itself well to Freenet, even in a Post-*Napster* world. Initially, proving end users' direct infringement (required for secondary copyright liability) was relatively easy in *Napster* and the ongoing *Grokster* litigation. By contrast, the previous section shows why proving copyright infringement by individual Freenet users is impracticable and complicated. Nevertheless, von Lohmann concludes that although a P2P system is protected by "plausibly deny[ing]" user infringement, the promotion, endorsement or aid in the infringing use of a P2P product may nonetheless potentially garner secondary copyright liability.[127]

[123] Freenet is released under the GNU (recursive acronym for "GNU's Not Unix") General Public License ("GPL"). *See* GNU, *Licenses*, *at* http://www.gnu.org/licenses/licenses.html (last visited May 8, 2002).

[124] Frank, *supra* note 3, at 8.

[125] Litman, *supra* note 49, at 167.

[126] *See id.*; however, Fred von Lohmann, an attorney for the Electronic Frontier Foundation ("EFF"), concludes that despite the lack of an actual case where "individual engineers or developers have been held personally liable for contributory or vicarious infringement, there is nothing in the law that would make this impossible. " *See* Fred von Lohmann, *P2P FAQ*, Electronic Frontier Foundation ("The vicarious and contributory infringement analysis detailed in the White Paper [on P2P copyright liability] applies equally to corporations or individuals. In several cases, for example, corporate executives have been held personally liable for vicarious or contributory copyright infringement alongside the companies that they manage."), *at* http://www.eff.org/IP/P2P/Napster/20010309_p2p_faq.html (last visited Nov. 2, 2002).

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

Proving the remaining elements of secondary copyright infringement against Freenet developers would be equally difficult. Vicarious liability does not really apply to Freenet. Vicarious copyright liability requires proof of a defendant's right and ability to control the copyright infringement of others and the derivation of a financial benefit from that infringement.[128] In *Napster*, the Ninth Circuit found that operating the central file-indexing server and running user accounts left Napster in control of its system.[129] In the *Grokster* case, the content industry alleges the defendants control their FastTrack systems through user accounts and rights to terminate users.[130] Freenet, by contrast, has no concept of outwardly identifiable "users" or any form of centralized control. Moreover, Freenet derives no direct financial benefit from the project, and its current developers obtain no obvious present or future financial gain from Freenet.

Claims for contributory liability might fare a little better, but would nonetheless prove difficult against Freenet. Contributory liability requires that the defendant had knowledge of and materially contributed to direct copyright infringement.[131] Knowledge can be demonstrated "by showing either that the contributory infringer *actually* knew about the infringing activity, or that he reasonably *should have known* given all the facts and circumstances (constructive knowledge)."[132] In *Napster*, actual knowledge was shown by company e-mails and monitored lists of thousands of infringing files.[133] Knowledge of Freenet developers would be difficult to prove based on evidence of monitoring files (like in the *Napster* case). However, if infringing files were found to be prominently listed on the Freenet, direct or constructive knowledge would be a feasible claim, especially given that infringing content largely comprises the current network.[134]

[128] *Id.*

[129] *See Napster*, 239 F.3d at 1023-24.

[130] NMPA, *Complaint, supra* note 83, at ¶ 67.

[131] *See* von Lohmann, *supra note* 128.

[132] *Id.*

[133] *See id.* Also, constructive knowledge was proven by the recording industry experience of Napster executives and inculpating "screen shots" used by Napster.

[134] *See* Jon Orwant, *What's on Freenet?*, OpenP2P.com (Nov. 21, 2000) (finding pornography, copyrighted MP3's, and unauthorized software), *at* http://www.openp2p.com/pub/a/p2p/2000/11/21/freenetcontent.html. In the author’s own experience, copyrighted Scientologist documents were easily found, and other content was too painfully slow to actually receive and/or confirm. The Freenet start page does link to "The Content of Nice" Freesite that links to pornography and scientology texts, as well as other sites. *See* The Content of Nice (this is a Freesite "link" and **cannot** be accessed directly from the WWW. Freeweb uses the end user's computer (127.0.0.1 is the home computer) as a proxy out into the secure Freenet), *at* http://127.0.0.1:8888/SSK%409G4s%7EjLQJB7ALQg-v2q5xKAJy9YPAgM/CoN//.

Additionally, Ian Clarke and other Freenet developers have publicly acknowledged the potential (and for some, the goal) of Freenet subverting copyright controls on file-swapping.[135] Proving material contribution to direct user infringement would likely be a straightforward claim against Freenet developers who offer the program to the public.[136] Thus, Freenet developers could conceivably face some form of contributory liability, although even such a finding still could not stop the Freenet network, or someone else from resuming their development roll.

The "substantial noninfringing use" doctrine (the "Betamax defense")[137] could be argued by any Freenet group claiming fair use protection for the "legitimate uses" of Freenet. Initially, Freenet is championed as a protector of free speech. Andrew Frank, writing for the content industry, even admits that "[l]egally, however, because their content is encrypted, [distributed, encrypted P2P systems] have a substantial non-infringing objective: to protect freedom of speech from censorship."[138] Although the copyright - free speech issue is a matter of ongoing debate,[139] it is conceivable that the core goal of the Freenet Project could be found to be a "substantial noninfringing use." Second, in the *Grokster* litigation, StreamCast has already indicated it believes that Morpheus has several substantial non-infringing uses (distributing public domain content, authorized software and media content, etc).[140] Any of these possible non-infringing distributions are possible on the Freenet as well. Third, Freenet is not necessarily an application that allows infringement, but a full "platform" in its own right.[141] An application, such as Freeweb (which allows a user to view websites over the Freenet) or

[135] The Freenet Project,*The Philosophy Behind Freenet* (last visited May 8, 2002) ("*You cannot guarantee freedom of speech and enforce copyright law*. It is for this reason that Freenet, a system designed to protect Freedom of Speech, must prevent enforcement of copyright." [emphasis in original]), *at* http://freenetproject.org/cgi-bin/twiki/view/Main/Philosophy (last visited Nov. 2, 2002).

[136] In *Napster*, the Ninth Circuit quickly affirmed the district court's holding that "Napster provides 'the site and facilities' for direct infringement[,]" by supplying the Napster program and central file-index server. *See Napster*, 239 F.3d at 1022.

[137] von Lohmann, *supra* note 128. This is von Lohmann's phrase for the defense.

[138] Frank, *supra* note 3, at 8.

[139] For a detailed discussion of the current conflict between copyright and free speech, *see* Ryan C. Fox, Comment, *Old Law and New Technology: The Problem of Computer Code and the First Amendment*, 49 UCLA L. REV. 871 (2002).

[140] StreamCast, *Motion for Partial Summary Judgment, supra* note 89, at 11-15.

[141] Cochran, *supra* note 38, ("'Comparing Freenet with Napster is like comparing Linux with Microsoft Word,' Clarke wrote on his website. 'Napster is an application, but Freenet is a platform.'").

Frost (which allows users to trade files over the Freenet) is required to actually perform any file-sharing.[142] While groups that develop these specific tools could face liability, the core Freenet network is likely legally immune because it does not actually swap files.[143] Fred von Lohmann concludes that when P2P technologies disaggregate functions in this fashion, they stand a much greater likelihood being of legally immune.[144] Fourth, the design choices of dynamically caching documents can be touted for their technological desirability, despite their hindrance to legal enforcement of copyrights. Caching and file distribution techniques save bandwidth, bring desired information more quickly to those who want it,[145] and provide free storage space for information.[146] Encryption of information guarantees data integrity against those who might attack communications. Additionally, the decentralized P2P system may prove more efficient at searching for information.[147]

Thus, the wide array of technological uses, free speech goals and potential for dissemination of "fair use," authorized, or public domain content leave Freenet in a better legal position than either Napster or the *Grokster* defendants. Nonetheless, the *Napster* decision (if followed by other circuits) has seriously limited the scope of the "Betamax defense" in the P2P context, and the mere copyright-subverting goal of Freenet could yield liability.[148] However, even if a court refuses to find "substantial non-infringing uses" of the Freenet system, the content industry will inevitably have to face the prospect of future P2P developers adopting these legally troubling designs as a standard, efficient approach to their new technologies.

[142] *See* The Freenet Project, *supra* note 39.

[143] Moreover, other, non-file trading utilities could provide evidence of substantial non-infringing uses. *See, e.g*. Everything Over Freenet, *at* http://eof.sourceforge.net/ (last visited Mar. 5, 2002).

[144] von Lohmann, *supra* note 128, ("This approach may also have legal advantages. If Sony had not only manufactured VCRs, but also sold all the blank video tape, distributed all the TV Guides, and sponsored clubs and swap meets for VCR users, the Betamax case might have turned out differently. Part of Napster's downfall was its combination of indexing, searching, and file sharing in a single piece of software. If each activity is handled by a different product and vendor, on the other hand, each entity may have a better legal defense to a charge of infringement.").

[145] *See* The Freenet Project, *supra* note 17; Oram, *Technological Innovation*, *supra* note 26.

[146] *See* The Freenet Project, s*upra* note 17, ("Universal personal publishing: Freenet enables anyone to have a website, without space restrictions or compulsory advertising, even if you don't own a computer.")

[147] *See* STUART BIEGEL, BEYOND OUR CONTROL?: CONFRONTING THE LIMITS OF OUR LEGAL SYSTEM IN THE AGE OF CYBERSPACE 289-90 (20012000) (noting that Gnutella's decentralized P2P architecture "could be the backbone of the next generation of search engines.")

[148] *See* von Lohmann, *supra* note 128.

Notwithstanding traditional secondary copyright liability, a group connected to Freenet could possibly try to seek refuge under section 512 of the Digital Millennium Copyright Act ("DMCA"), but would not likely be successful.[149] Section 512, the "safe-harbor" provision, provides "online service providers" with four bases of protection, covering: "[t]ransitory communications[,]" "[s]ystem caching[,]" "[s]torage of information on systems or networks at direction of users[,]" and "[i]nformation location tools."[150] However, von Lohmann notes that because "Congress did not anticipate peer-to-peer file sharing when it enacted safe harbors, many P2P products may not fit within the four enumerated functions." Von Lohmann posits that the transitory communications exception[151] would not apply unless the network traffic actually passes through the P2P's private network.[152] Napster failed under this standard, and Freenet clearly would as well, given that Freenet has no "private" network of its own.[153] Although the "system caching" exception[154] seems to encompass Freenet, this and the remaining two exceptions all require some form of blocking access to or taking down information upon notification of copyright infringement.[155] The Freenet system is thus problematic under DMCA safeguards because it deliberately prevents the forcible takedown of information.

Additionally, any group of Freenet developers sued by a plaintiff would likely have difficulty proving they are an "online service provider" ("OSP").[156] To qualify for any of the safe harbor protections, an OSP must terminate users who infringe copyright laws and not interfere with “standard technical measures” that protect copyrights.[157] Freenet does not employ a "user" system; the very design of Freenet as a censorship resistant technology could be seen as an interference with “standard technical measures.”[158] Also, von Lohmann notes that an OSP "must not have known about the

[149] 17 U.S.C. § 512 (1998); *see also* von Lohmann, *supra* note 128.
[150] U.S. Copyright Office, *The Digital Millennium Copyright Act of 1998, U.S. Copyright Office Summary* at 8 (Dec. 1998), *available at* http://www.loc.gov/copyright/legislation/dmca.pdf.
[151] 17 U.S.C. § 512(a) (1998).
[152] von Lohmann, *supra* note 128.
[153] *Id.*
[154] 17 U.S.C. § 512(b) (1998).
[155] Copyright Office, *DMCA Summary, supra* note 151, at 11-13.
[156] von Lohmann, *supra* note 128.
[157] 17 U.S.C. § 512(i)(1) (1998); von Lohmann, *supra* note 128.
[158] von Lohmann, *supra* note 128. Also, an OSP must designate a "copyright agent" to formally accept notices of infringement by copyright owners, register with the Copyright office and place contact information on their web site. *See id.* The Freenet Project web site provides no such notice or agent, and

infringement, or been aware of facts from which such activity was apparent (i.e., if you take a 'head in the sand' approach, you lose safe harbor)."[159] The developers of Freenet would likely be found to have at least constructive knowledge of copyright infringement.[160] Alternately, if the content industry attempted to sue internet service providers ("ISP's") (such as America Online, etc.), for merely allowing users to run Freenet nodes, it is likely that such ISP's would qualify as OSP's and fall within one of the safe harbor categories.[161] However, for any group directly connected to Freenet, and merely aiding a Freenet project, the DMCA safe harbor protections would likely be unavailable.

C. **Prospective Legal Approaches to Evolving P2P Technologies**

The P2P legal landscape has been continually changing since *Napster*. As the content industry moves forward in its litigation with the FastTrack P2P companies, the FastTrack system may prevail where Napster failed because its service is more decentralized and encrypted than Napster. Furthermore, if the content industry does succeed in the *Grokster* litigation, P2P developers will move on, trying to create a system that cannot be stopped by copyright law.

Some observers have suggested that the DMCA could be amended to require ISP's or individual users to only allow P2P technologies over their networks that respected copyrights.[162] Freenet developers have even pondered Freenet specific

there is likely little point for any Freenet project to designate such an agent, given the inability to forcibly take down copyrighted material. *See* The Freenet Project*.*, *supra* note 5.

[159] *von Lohmann, supra* note 128.

[160] Due to the statements about copyright on their website and previous press statements, detailed in previous analysis.

[161] ISP's *can* terminate "users," by terminating whole accounts, and are the actual aim of the 512 protections.

[162] *See* Strasser, *supra* note 2, at 710 (suggesting to amend Section 512 to "require that ISPs who wish to qualify for one of the statutory safe harbors use technologies that enable the government to enforce copyright law."); Damien A. Riehl, Article, *Peer-To-Peer Distribution Systems: Will Napster, Gnutella, And Freenet Create A Copyright Nirvana Or Gehenna?*, Electronic Commerce in the 21st Century, 27 WM. MITCHELL L. REV. 1761, at 1788 (2001) (noting that "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.").

legislation or litigation that would impose burdens on individual Freenet nodes.[163] However, such approaches would likely run afoul of the current "no mandate" technology provision of the DMCA[164], and restrain technological innovation too greatly to be palatable options.[165] Moreover, Freenet (or other P2P) communications may eventually become so well-masked and undetectable that legal action would be practically moot.[166]

In the meantime, the content industry has not been waiting idly for the day when the existing copyright framework falters under technological advances. In addition to attempting to thwart existing P2P networks,[167] the content industry has begun to push the government for stronger copyright controls on the user's end.[168] Damien Cave observes the broad scope of the content industry's vision:

> Hollywood is on the march. Adding copy protection to CDs is just one tactic in a comprehensive onslaught. Media behemoths like Disney, Sony and AOL Time Warner are seeking full control of all methods of entertainment distribution; if their vision is realized, digital television sets, hard drives, personal video-recorders and wireless devices will all have some form of copy protection. In the most dire incarnation of the digital entertainment future, consumers of music and movies won't be able to make any copies at all without explicit permission...[169]

The content industry is seeking the help of the government to force users away from "insecure" medium to copyright-owner friendly technologies.[170] This approach, also called "digital rights management" ("DRM"), aims to simply make it impossible for any individual to play unauthorized content on their computer or device.[171] The Consumer Broadband and Digital Television Promotion Act ("CBDTPA"), proposed by Senator Ernest Hollings at the behest of the content industry, would simply bypass the P2P threat

[163] Posting of Timm Murray, tech@freenetproject.org, to [freenet-tech] listserv (July, 29 2001) [freenet-tech] ("Consider what happened with Napster. If they do not filter searches, they are legally liable for contributing to copyright infringement. What I am asking is why is it unlikely that the RIAA would not publish a list of CHK's that all node operators must not pass."), *available at* http://hawk.freenetproject.org/pipermail/tech/2001-July/000795.html.

[164] 17 U.S.C. § 1201(c)(3). (Supp. 2002) (1998).

[165] *See* Riehl, *supra* note 163, at 1788-89 ("Even if the legislation were drafted broadly enough to cover these latter technologies, it would likely be too restrictive - and would constrain technological advances.").

[166] Clarke*, supra* note 27.

[167] King, *supra* note 26.

[168] *See* Damien Cave, *Chained Melodies*, Salon.com, (Mar. 13, 2002), *at* http://www.salon.com/tech/feature/2002/03/13/copy_protection/index.html.

[169] *Id.*

[170] *Id.*

by requiring all computers and digital devices to ensure that only authorized copyrighted content could be accessed.[172] Although the CBDTPA has not made measurable progress in the Senate at the time this article was written, the content industry is steadily moving along with a mixed technology-legislation DRM approach. If successful, all existing P2P systems would cease to be a copyright threat if their unauthorized content could not be used on the end user's computer. Not without its critics, DRM has been harshly criticized for putting far too much power over information in the hands of the content industry.[173] Additionally, many observers note that the DRM approach may alienate too many consumers, as well as ultimately prove technologically impossible.[174]

D. **Prospective Non-Legal Approaches to Evolving P2P Technologies**

Should the current regime of copyright law fail to stop Freenet, content owners or the legal system could attempt to technologically attack or poison the system.[175] Nevertheless, this threat has been assumed from the start, and the Freenet Project maintains that it can only be shut down when the Internet is turned off.[176] Architectural changes in the Internet could make this more feasible, however. Lawrence Lessig contends that the Internet as a whole is moving away from being a "stupid" network that is difficult to control to a "smart" network that will be more readily manipulated by powerful corporate and government actors.[177] Although a remote threat as pertains to Freenet now, things change very quickly on the Internet. Such architectural change could eventually control the Freenet, which currently relies on the nondiscriminatory flow of data in the current "stupid" network design to hide and secure the Freenet network.

If both the technological and legal arenas fail to stop P2P systems like Freenet, the content industry may have to reconsider its approach towards P2P technologies.

[171] Michael Fraase, *When Elephants Dance*, Arts & Farces internet (Mar. 23, 2002), *at* http://www.farces.com/comments.php?id=P53_0_1_0_C and requires registration (last visited Oct. 25, 2002).

[172] *Id.*

[173] *Id.*

[174] *Id.*

[175] For further discussion of physical attacks against the Freenet, see Clarke, *supra* note 33.

[176] Heyman, *supra* note 19 (quoting Clarke: "I can't envision a way to shut down Freenet without shutting down the Internet").

Professor Litman argues that content industry must take steps beyond their current legal and technological strategies:

> If forty million people refuse to obey a law, then what the law says doesn't matter. It may be that people flout it because they're natural lawbreakers, or it may be ... that they don't comply because it doesn't make sense to them. Whatever the reason, the law is not going to work well in the real world.[178]

Professor Litman concludes that this is simply the age-old tradition of copyright owners resisting all new forms of technology they cannot control.[179] Talal Shamoon, executive vice president of InterTrust, a company pioneering copy-protection strategies for the content industry, acknowledges that the P2P controversy illustrates an "ugly transition period" in the digital revolution.[180] Nonetheless, Shamoon believes that regardless of a particular solution, the content industry will adapt to the specter of P2P technologies and other advances.[181] As it turns out, Ian Clarke would agree with Shamoon's assessment: "Artists and publishers all adapted to those new technologies and learned how to use them and profit from them; they will adapt to Freenet as well."[182]

Conclusion

More legal questions and conundrums are raised with a technology like Freenet than can be currently answered. Presently, Freenet is still an enthusiast's toy and not the "next" or current Napster, Morpheus, etc. However, even if Freenet never gains a massive user base, the law-defying encryption and distributed caching techniques of the project will likely end up in the next generation of P2P services. The struggles over changes in the Internet, seen through the eyes of emerging technologies, demonstrate that the confrontations between copyright owners and free information advocates will only continue to escalate. This escalation will be inextricably tangled in both legal and

[177] *See* Lawrence Lessig, The Future of Ideas 35-48, 267 (2001).

[178] Litman, *supra* note 49, at 114.

[179] *Id.* (observing that in dealing with new digital technologies, "[c]urrent stakeholders, who are used to the current rules, would of course prefer that the rules that apply to the general public engaging in these activities be the current rule, or ones that work as much like them as possible.").

[180] Cave, *supra* note 169, at 4.

[181] Markoff, *supra* note 34.

[182] *Id.* (quoting Clarke).

technological complexity, as neither the law nor technology appears capable of solving these dilemmas alone.

As Andrew Frank poignantly observes, P2P technologies are evolving in a "Darwinian" fashion, proving more resistant to technological and legal control with each iteration.[183] The content industry stopped Napster. The industry may stop the FastTrack companies. It may even stop Freenet. Eventually, however, a new system, borne of the lessons of these pioneering technologies, will likely arrive that cannot be addressed within the current practical confines of copyright law. When that day comes, the content industry will perhaps have to consider (if has not already done so) how it will "evolve" in the ever-changing digital landscape.

[183] Frank, *supra* note 3, at 38.