

Steal This Intellectual Property:
The Appellate Courts Grapple with the
Online File-Sharing Revolution

*Robert Khuu, Charlene Leus, Helen Sul & Long T. Tran**

INTRODUCTION

Imagine an apartment complex. Now, imagine a person has rented out one of the apartments for the purpose of setting up a drug dealing operation. Of course, the landlord has no knowledge of this. In fact, the landlord is legally bound to *not* intrude upon the tenant's privacy. As such, the landlord cannot be held liable for what the tenant is doing inside the apartment. This parallels very closely to the notion of indirect liability for of peer-to-peer file-sharing. In the peer-to-peer (P2P) context, a software provider gives users access to an environment that allows for the online trading of electronic files with other users; the provider is not actively trading any copyrighted files, but the users might be. The software provider is merely granting access to the facilities.

Arguably, whether or not the user actually uses the software for legal or illegal purposes is not the "software industry's" concern nor should it be; however, the "content industry" (i.e., the Recording Industry Association of America, the Motion Picture Association of America, as well as individual artists and authors) is asking the courts to hold these software companies liable for their users' actions. Why would the content industry take on the growing software industry over the actions of individual users? The answer is simple: digital media can be copied and traded on such a massive scale, by any

* Robert Khuu majored in Political Science and graduated from UCI in June of 2005. While at UCI, Robert served the Law Forum Journal as an editor, lead editor and contributing author. Charlene Leus, also a June 2005 UCI graduate, majored in Sociology with a minor in Political Science. Helen Sul majored in Political Science with a minor in Management, graduating from UCI with honors in June of 2004. Long T. (Lynne) Tran, also a June 2004 UCI graduate, majored in Political Science with a minor in Management. Charlene is currently a first year law student at the Regent University School of Law in Virginia. Robert and Lynne also plan to attend law school, while Helen is working in the in-house legal department of a company in the aviation industry and considering several graduate school programs.

individual user, that the content industry is facing the greatest threat to control of its product it has ever known. Whether by incident or by design, the software industry is facilitating this threat.

As a result of this clash, software and information technologies can develop in two directions: one where software is bound by heavy legal requirements or the other where information and software flow freely, uninhibited by legal requirements. However, both of these extremes are undesirable, because over-regulation will hamper innovation and under-regulation will breed piracy. After introducing the relevant legal standard and recent caselaw in more detail, this article will present the argument that the law must take advancements in computing technologies into account. A proper legal groundwork must be created in to order respect the social benefits provided by both the content and software industries. As the appellate courts grapple with this issue, and issue what might be viewed as conflicting rulings, at least one case is making its way to the United States Supreme Court. This article will conclude by challenging the notion that the Supreme Court simply 'must' intervene with more aggressive copyright liability for software providers.

BACKGROUND

Intellectual Property Owners: The Music Industry Example

The commercial music industry has played an instrumental role in the advancement of the arts by consistently contributing creative works of music for society to enjoy. There are multiple players involved in producing a musical work: songwriters, artists, musicians, and record companies. These parties commit substantial amounts of time and effort in order to produce a musical work. As contributors to our culture, they are rewarded for their efforts with legal rights of ownership for their creative works.

The recording arm of the music industry has long been associated with large studios such as Sony Music Entertainment Inc., Interscope Records, and BMG Music. A rewarding deal with a major record label could, in the case of a successful album or CD, yield profit from royalties for years to come – in addition to fame and fortune. The legal right to control this “intellectual property” (in the form of copyright) guarantees that the musician, lyricist and recording studio involved will reap the profits associated with their musical creation. The creation of a musical piece is a work of art that involves not only the musician, but the record company, musical writers, lyricists, background

**University of California
Irvine
Law Forum Journal**

Vol. 3

Fall 2005

singers, and a plethora of other parties whose contributions to the work often go unrecognized by the public. While the creation of a musical piece involves artistic contributions from multiple parties, it is the recording studio that must absorb the cost and potential risks associated with the investment in a project. The people associated with the content of a song are usually paid by the recording studio, which in return yields its profits from the sale of the recording in question.¹

In order to understand what is at stake in this process for the record companies, it is important to understand the various costs that are involved in producing a music CD.² Record companies spend considerable amounts of money in order to discover and develop recording artists. While there is no guarantee that they will actually see any return from their investment, major record companies spend, on average, roughly \$500,000 to \$1,000,000 in order to begin marketing a new artist.³ Record companies also incur the costs of manufacturing and packaging the CDs. Further, there are the high costs of advertising and promoting the CD on television, radio, and in print media. In addition to these costs, record companies must make periodic payments to the recording artists, the back-up musicians, various trust funds, technicians, and other staff personnel involved in the process.⁴

In exchange for their creative efforts and investment, the artists and the recording studios own copyrights to the work. The 1976 Copyright Act states that “musical works, including any accompanying words... [and] sound recordings”⁵ are protected as intellectual property.⁶ Musical works are divided

¹ Courtney Love, *Courtney Love does the Math*, Salon.com (2000), at <http://dir.salon.com/tech/feature/2000/06/14/love/index.html> (visited August 2005).

² At the time of this writing, the digital “compact disc” recording format (commonly referred to as a ‘CD’) is the most common method of commercial music distribution.

³ Lynn Morrow, *The Recording Artist Agreement: Does it Empower or Enslave?* 3 Vand. J. Ent. L. & Prac. 42 (2001).

⁴ Payments to artists, with the exception of royalties on particularly popular songs, usually take the form of ‘advances’ that will be recouped by the studio (with luck) from the sale of the recording. Russell J. Frackman, on behalf of Mitchell Silberbert & Knupp, LLP, attorneys for A&M Records et al., Complaint for Contributory and Vicarious Copyright Infringement, A&M Records et al. v. Napster (filed December 1999) at 3.

⁵ 17 U.S.C. § 102 (a)(2)(7) (1976).

⁶ The protection of copyrights is unlike that of any other tangible object. Copyrights are not tied to any physical manifestations so file traders are not “taking” physical

into two major components: (1) the musical composition and its performance, and (2) the actual sound recording created at a specific point in time. The sound recording itself is considered a creative work due to the vast number of choices made in mixing the various components of the work. Therefore, the songwriter and performers hold copyrights to the composition and its performance, while the recording studio holds a copyright in the sound recording.⁷

With the emergence of the “Information Revolution” and the development of the microprocessor, the landscape of copyright protection inevitably changed. The most notable achievement in computer technology was the emergence of the Internet as a public medium in which information could freely be exchanged. The Internet allows for the building of online communities where individuals can exchange digital data with one another. Various types of digital media can be exchanged over the Internet: text documents, movies, music, and pictures are common examples. This promoted

objects when they download music without authorization. Copyright owners own a “bundle of rights” by virtue of their creation, rather than own the work in its entirety, which is defined by the Copyright Act. The Copyright Act provides:

Subject to sections 107 through 12(2), the owner of copyright under this title has the exclusive rights to do and to authorize any of the following:

- (1) to reproduce the copyrighted work in copies or phonorecords;
- (2) to prepare derivative works based upon the copyrighted work;
- (3) to distribute copies or phonorecords of the copyrighted work to the public by sale or other transfer of ownership, or by rental, lease, or lending;
- (4) in the case of literary, musical, dramatic, and choreographic works, pantomimes, and motion pictures and other audiovisual works, to perform the copyrighted work publicly;
- (5) in the case of literary, musical, dramatic, and choreographic works, pantomimes, and pictorial, graphic, or sculptural works, including the individual images of a motion picture or other audiovisual work, to display the copyrighted work publicly; and
- (6) in the case of sound recordings, to perform the copyrighted work publicly by means of a digital audio transmission.

17 U.S.C. 106 (1994 & Supp. 1999).

⁷ Lamberto O. Abeleda, Jr., *Digital Compensation: Recording Artists’ Collective Fight for True and Fair Compensation*, 31 Sw. U. L. Rev. 703 (2002).

the creation of software that facilitates the transfer of electronic media over the Internet in an easy and efficient way, commonly referred to as peer-to-peer (P2P) file-sharing software.

The purpose of P2P technology is to enable users to share digital media through the Internet with other users. A user is able to search for a file by name and download the file from one or more users who have a copy of that file on their computers' hard drives. This technology easily facilitates the transmission of information and media over the Internet, thereby enabling individuals to illegally exchange copyrighted works as well. Everything from copyrighted movies to copyrighted music began to travel across the Internet. With the creation of the digital medium, a copy of a file could be continuously reproduced and transmitted between users, and the quality of the file would never decline significantly. This made digital files much more difficult to control than their predecessors – analog copies of radio or television transmissions that decreased significantly in quality with every copy and required physical delivery to a new user. With digital technology, one individual could create an infinite number of *perfect* copies of the protected work at no cost and share these copies instantly with the world at large.

Sharing is the problem. An old-fashioned analog tape recording is usually only available to a small number of people; however, with digital recordings, P2P software and access to the Internet, a user can literally share the music file with the entire world. This technology allows for the creation and distribution of multiple copies of a copyrighted file to an unlimited audience, thus creating a situation in which the recording companies are less able to sell CDs and control the distribution of the copyrighted music. The universal love for music, combined with the convenience and simplicity provided by the P2P file-sharing system soon became an explosive combination and the driving force behind a public that felt music ought to be free. Music sharing went from just a new hype to becoming a part of mainstream culture; P2P file-sharing services were soon boldly advertised on television. It became a norm for the public to expect 'free' music regardless of the fact that such sharing usually violated copyrights.

Copyright law creates an incentive for the recording studios to invest in an artistic venture. The public stigma against the music industry as a self-serving billion-dollar magnate often did not take into account the fact that this industry provides the economic foundation for many people whose livelihood

depends solely on the sale of music.⁸ Due to this stigma, many users feel very few qualms when it comes to downloading and infringing the ‘wealthy’ industry’s copyrights. The content industry soon discovered how difficult it was to catch individual users in the act of sharing; instead, the industry began to concentrate its legal attack on more identifiable targets – the P2P software providers.

Therefore, technological advances have raised the core legal question at issue in such cases: Can the provider of an online P2P file-sharing service or a P2P software program be guilty of secondary liability for copyright infringement based on the actions of its users? The recording studios, joined by many musicians and lyricists, argue that the Courts must interpret secondary copyright law in a manner that will prevent future P2P sharing of copyrighted works. The P2P providers, joined by many sympathetic supporters, argue that such a restrictive reading of copyright law would stifle valuable technological innovations. Should courts hold the providers of P2P file-sharing software or services liable for the illegal file exchanges? Thus far, some judges have answered this question in the affirmative; however, other judges have found reason to exonerate certain P2P providers. While one of the cases appears to be headed to the United States Supreme Court,⁹ this article provides a survey of several appellate courts’ reasoning. Following this survey of notable cases, this article proceeds with an analysis of the need (or lack thereof) for aggressive judicial intervention in this area.

The Napster Case

Originally a software program created by a Northwestern University undergraduate student named Shawn Fanning to share music with his peers, within a matter of years the *Napster* P2P file-sharing service had a user base of millions of people worldwide. Once established online, Napster provided free *Music Share* software from its website for users to exchange music files.¹⁰ The

⁸ A & M Records, Inc. et al. v. Napster, Inc., 239 F.3d 1004, 1036 (9th Cir. 2001).

⁹ See the discussion of the *Grokster* case later in this article. The parties to the *Grokster* case have delivered their arguments, dozens of amicus curie briefs have been filed, and as of this writing, the Justices of the Supreme Court have yet to render a decision.

¹⁰ Russell J. Frackman, on behalf of Mitchell Silberbert & Knupp, LLP, attorneys for A&M Records et al., Complaint for Contributory and Vicarious Copyright Infringement, A&M Records et al. v. Napster (filed December 1999) at 5.

simplicity and convenience of Napster's technology made P2P music sharing incredibly popular. Napster was serving millions of users worldwide until 2000, when it was sued by the recording industry and various artists. By this time Napster had become the most popular P2P system on the Internet; users around the world traded a hundred or more music files per second. What had originated as a forum to exchange music made by friends developed into a global marketplace for pirated music.

The Napster Technology

The Napster software allowed users to connect their computers to a hub of computer servers maintained by Napster and interact with other software developed and maintained by Napster on its computer servers.¹¹ To begin, users registered with Napster by providing a user name, but the disclosure of their real name and personal information were optional. By providing the option of anonymity, Napster became one of the most popular websites on the Internet. The recording studios alleged that Napster attempted to protect its users' privacy and anonymity in order to conceal copyright infringement from being exposed: "Users [would] understand that they [were] improving their experience by providing information about their tastes without linking that information to a name or address or other sensitive data that might endanger them."¹²

P2P file-sharing systems became extremely popular with the introduction of MP3 files. MP3, which is an abbreviation for Moving Picture Experts Group Audio Layer-3, is a compression system used to compress sound and it is the standard format used to store digitally compressed files. Unlike CD reproductions which easily can use up 60 megabytes of space per recording,¹³ MP3 is digital music that can be compressed to one hundredth of the original CD storage size and can be transferred easily over the Internet.¹⁴

¹¹ *Id.* at 5.

¹² Russell J. Frackman, on behalf of Mitchell Silberbert & Knupp, LLP, and Carey R. Ramos, on behalf of Paul Weiss Rifkind Wharton & Garrison, attorneys for A&M Records et al., Joint Motion for Preliminary Injunction, A&M Records et al. v. Napster (filed June 12, 2000) at 1.

¹³ Eugene Quinn, *Only Themselves to Blame*, Jurist (2005), at <http://jurist.law.pitt.edu/forum/forumnew127.php>.

¹⁴ MP3 is a compression technology that reduces the file size of a sound recording to a ratio of 12:1 and "allows for the fast and efficient conversion of compact disc

**University of California
Irvine
Law Forum Journal**

Vol. 3

Fall 2005

Audio CDs can be ‘ripped’ onto a computer and compressed into this much smaller file without any degradation to its initial quality; it is a near perfect reproduction of the original no matter how many times copied.¹⁵ Due to the small size of the file, MP3 has been the optimal format to use when trading songs over the Internet since it consumes very little hard drive space and can be downloaded in a matter of minutes.

After registering on the Napster website, users were able to download the free software that was required to use the Napster program. Using the software’s search engine feature, a user could search for the file name of a song she wished to download.¹⁶ When a user entered the name of a song she wanted, the Napster system searched its central indices for the file name and sent back a list of matching results. After reviewing the list of search results, a user chose the song that she wished to obtain (and the specific host she wished to obtain it from) by clicking on the name of the file. With a click of the mouse, Napster’s server connected the user and the host so that the user could download the song directly from the hard drive of the host.¹⁷ Users could even build a library of favorite hosts, and easily check to see what other files that host might have available for sharing.

In addition to helping users locate the music file, the Napster software was ‘intelligent’ and would keep track of the file that the user was trying to download. In the event the uploader¹⁸ signed off in the middle of the transfer or the file was somehow no longer available, the software would locate a similar

recordings into computer files that may be downloaded over the Internet.” *A & M Records, Inc., et al. v. Napster, Inc.*, 114 F. Supp. 2d 896, 897 (N.D. Cal. 2000).

MP3 utilizes a method of file compression known as Perceptual Audio Coding. This process strips away digital information that is inaudible to the human ear and shaves off much of the unnecessary sound data from the digitized format. Alex Colangelo, *Copyright Infringement in the Internet Era: The Challenge of MP3*, *Alta. L. Rev.* 3 (Apr. 2002).

¹⁵ The process of ripping a recording file onto the computer to transforming it into digital MP3 format is not a part of the Napster system. Ripping a file is the precursor to use the Napster software and share music.

¹⁶ ‘Downloading’ refers to the process of copying a file found on the Internet or another user’s computer to one’s own computer.

¹⁷ Russell P. Beets, *Note and Comment: RIAA v. Napster: The Struggle to Protect Copyrights in the Internet Age*, 18 *Ga. St. U. L. Rev.* 518 (2001).

¹⁸ ‘Uploading’ refers to the process of copying a file found on the user’s own computer to another destination, such as the Napster server or another user’s computer.

file with the desired quality and features and proceed seamlessly with the download. Napster claimed that its users could always find what they were looking for by using its system. Throughout the sharing process, Napster's server operated automatically. No actual human beings ever screened the files or user transactions.

The Music Share software enabled users to connect to Napster's central indexing server. Through the very nature of peer-to-peer technology, Napster itself never stored copies of the songs on its central server; rather, Napster's central server only functioned as an index system that compiled indices of MP3 file names made available to users upon request. Once a user successfully logged on, the server verified whether she had consented to share her files with other users. Each user had the choice of allowing her files to be shared with others or not. If the user had set up her account to allow sharing, all the files in her user library were automatically made available to other online Napster users.

Napster's central index was comprised of millions of file names made available by such individuals. Since individual users designated the names for these files, they often contain spelling errors or displayed inaccurate descriptions of the file's content. It is important to note that Napster did not have access to the content of the files. As a result, it was not possible for Napster to screen the content of the files. Napster only verified that the file was in the correct MP3 format to be downloaded: Napster's primary function was to connect users to each other, and once the connection was made Napster did not interfere with the trading process.¹⁹ Moreover, the file indices were "fluid," meaning that the server only tracked those users who were connected to the network in real time.²⁰ Thus, Napster never maintained a permanent directory of file names that were available for sharing.

During this period Napster did not charge a fee to its users; the majority of its revenues came from advertisers who paid according to the number of users that viewed the site and saw the banner ads. During each log on, users were exposed to advertisement banners integrated into the browser interface. This concept of reaching the most people was a reasonable motive for Napster to expand its user base because the more people that viewed the site and saw the ads, the more money those advertisers were going to pay to Napster.

¹⁹ Russell P. Beets, *Note and Comment: RIAA v. Napster: The Struggle to Protect Copyrights in the Internet Age*, 18 Ga. St. U. L. Rev. 545 (2001).

²⁰ *Napster*, 114 F. Supp. 2d at 898.

In addition to the file-sharing service, Napster provided a number of other services that did not entail the trading of copyrighted materials. The chat-room service provided users the opportunity to chat with other users online. Through Napster's chat room service, users were able to communicate in groups categorized by various genres of music. It was the perfect medium for music lovers with similar music interests to communicate with one another.²¹

Like the chat room, the New Artist Program promoted communication among music-lovers and it also provided new artists with an effective way to distribute and promote their music to the public. Through the New Artist Program, emerging bands were able to reach out to interested fans and inform them about band news and upcoming events. When a user wished to sample the new artist's music, she would download the band's music using the same method necessary to obtain any other file on the Napster network. As with all other files, a user had to utilize Napster's search engine to search for and download the new artist's music. Thus, the system was, in such cases, used for the legally approved download of copyrighted music.

Since users were able to create pseudonymous usernames and passwords, they were able to remain anonymous to other users and even Napster's operators. Thus, there was virtually no way for Napster keep detailed records of any potential copyright infringement. Napster, however, did retain the right to terminate access to users through the user agreement. Users were required to agree to a Terms of Use contract upon sign-up, which granted Napster the right to block the access of users engaging in unlawful conduct.²² However, the user agreement soon became an ineffective method of banning unauthorized users, as simple tips on how to obtain a fresh username circulated throughout the Internet.²³

²¹ Lior Jacob Strahilevitz, *Charismatic Code, Social Norms, and the Emergence of Cooperation on the File-Swapping Networks*, 89 Va. L. Rev. 512 (2003).

²² In fact, Napster regularly took disciplinary action and terminated access to users exhibiting inappropriate behavior. Russell P. Beets, *Note and Comment: RIAA v. Napster: The Struggle to Protect Copyrights in the Internet Age*, 18 Ga. St. U. L. Rev. 545 (2001).

²³ Frank Bourbon, *Hard on the Street*, ZDNer Music (2000), at <http://ankarino.tripod.com/frankb/frankbourbon5.html>.

Contributory Copyright Infringement

Napster quickly became a popular site for users to enjoy free music. However, this negatively affected music copyright owners who were furious that their music was being downloaded without compensation. In late 1999, the Recording Industry Association of America (RIAA) sued Napster for copyright infringement. The lawsuit demonstrated to the public that the music industry would not tolerate piracy and would aggressively pursue copyright infringers. More than a dozen recording studios, independent artists, and those involved in the process of making musical recordings accused Napster users of actively participating in the illegal reproduction and distribution of music.²⁴ These plaintiffs sought to shut down the P2P revolution at its source, by obtaining a ruling that Napster was secondarily liable for the illegal behavior of its users through both *contributory* and *vicarious* copyright infringement.

The elements of a claim for contributory and vicarious copyright infringement have some overlap, and some important differences. First, to establish *contributory* infringement, the plaintiffs needed to prove:

- (1) A direct infringement (by Napster's users) occurred;
- (2) The defendant (Napster) knew or had reason to know of the infringing activity; and
- (3) The defendant (Napster) induced, caused, or materially contributed to the infringing activity.²⁵

Contributory Element #1: Third Party Infringement

The claim of contributory copyright infringement did not charge Napster with the *direct* violation of copyright law, but instead, sought to hold the company responsible for the illegal activity of its users. According to the plaintiffs, although Napster creators did not *themselves* pirate music, Napster had created a forum that enabled *users* to more easily infringe. A copyright gives the owner of the intellectual property the right to control the distribution and reproduction of a work. When users are downloading music onto their computers, they are making an illegal reproduction because they do not have the permission of the copyright holders. Secondly, users also violate copyright law when they distribute the music to others without permission. Each of these

²⁴ *Napster*, 114 F. Supp. 2d at 897.

²⁵ *Id.* at 901.

violations of the exclusive rights granted to the copyright owners can be the basis for a claim of direct infringement by Napster users.

Napster counter-argued that its users were making 'fair use' of the plaintiffs' music -- a defense sanctioned (in certain situations) under the Copyright Act. The District and Appellate Courts disagreed,²⁶ finding that Napster's users were not 'fair users,' and thus they were directly infringing on copyrighted music. Therefore, since the courts viewed Napster's users as copyright infringers, the first element for a claim of contributory infringement against Napster had been satisfied.

Contributory Element #2: Knowledge

The knowledge element of contributory copyright infringement can be based on two forms: *actual* (based on proof of knowledge) and *constructive* (based on evidence suggesting the party 'should have known'). Constructive knowledge can be somewhat easier to prove than actual knowledge; the mere design of a product or system might lead to the argument that its creator 'should have known' of the potential for copyright infringement. However, awareness of possibility for abuse by creators of a new technology, by itself, is not necessarily enough to show knowledge of infringement according to the *Sony Betamax* case. In *Sony Corp. of America v. Universal City Studios, Inc.* [Sony Betamax],²⁷ the Supreme Court ruled that Sony could not be held liable for contributory copyright infringement simply because it sold a machine -- the 'Betamax' video tape recorder -- that could theoretically be used to infringe copyrights.

The Court reached this conclusion based on evidence that the product could also be used for "substantial non-infringing uses," such as the recording of religious or sports programming that was freely offered for sharing by the copyright owners. The Court did not, however, articulate clear guidelines as to what makes the non-infringing use of a new technology *substantial*. Thus, for many years since, the substantial non-infringing uses defense to the *constructive knowledge* element of contributory infringement has been

²⁶ For a detailed discussion of the 'fair use' defense and the Napster Courts' reasoning, see Hu, Leus, Tchobanian and Tran, *Copyright vs. Napster: The File Sharing Revolution*, 2 UCI L. Forum J. 53 (Fall 2004), available online at <http://www.socsci.uci.edu/lawforum/content/journal>.

²⁷ *Sony Corp. of America et al. v. Universal City Studios, Inc. et al.*, 464 U.S.417 (1984).

available to the creators of new technology, but without further clarification by the Supreme Court as to its limits.²⁸

When allegations were made that Napster had *constructive* knowledge that its system was being used for massive copyright infringement, Napster did indeed raise the *Sony Betamax* defense. Napster argued that although, in theory, its system could be used for copyright infringement, the system could also be used for ‘substantial non-infringing uses.’ Napster provided evidence that several music artists, who were often unrepresented by recording studio contracts, wanted users to freely exchange their music. For them, Napster was a new way of promoting their music, and as the copyright owners to their music and their sound recordings, they approved of this copying and distribution.²⁹

The District Court did not devote a great deal of time to discussing whether Napster had proved that the non-infringing use of its system was ‘substantial’ enough to defeat an allegation of *constructive knowledge*. Instead, the Court accepted the plaintiffs’ evidence of *actual knowledge* of infringement by Napster’s users. Napster had failed to respond to the music industry’s threat of legal actions: ‘Plaintiffs, through the RIAA, notified Napster in writing of the massive infringing activity taking place on its service, including specific notice of over 12,000 infringing MP3 files.’³⁰ The plaintiffs sent Napster written warnings demanding the removal of numerous represented artists and their music from Napster’s system. Napster failed to employ any sort of automated filter on the system after receiving lists of protected songs.³¹

Napster argued against the use of this evidence as well, claiming that the lists were insufficient in detail to tailor a reasonable filter accordingly. Napster also claimed that the vast number of trades taking place on the system made it impossible to keep up with copyright ownership. By the time the case reached the Court of Appeal, the burden was placed on the music studios to provide more specific lists of artists and song titles that were protected.

²⁸ Lee Burgunder, *Reflections on Napster: The Ninth Circuit Takes a Walk on the Wild Side*, 39 Am. Bus. L. J. 684 (2002).

²⁹ *Napster*, 114 F. Supp. 2d at 901.

³⁰ Russell J. Frackman, on behalf of Mitchell Silberbert & Knupp, LLP, and Carey R. Ramos, on behalf of Paul Weiss Rifkind Wharton & Garrison, attorneys for A&M Records et al., Joint Motion for Preliminary Injunction, *A&M Records et al. v. Napster* (filed June 12, 2000) at 13.

³¹ *Napster*, 114 F. Supp. 2d at 901.

However, this was not a complete solution to the problem.³² Since users named their own files, Napster could not always ascertain which files actually matched artist and song names provided by the plaintiffs. Sure enough, once Napster eventually implemented an electronic filter to prevent trading of songs from the plaintiffs' lists, Napster users quickly began working around the filter by renaming their music files with misspellings or code names. Thus, once again, the technology involved made it difficult to pin the concept of *actual knowledge* of infringement on Napster.

In the end, Napster was not able to defend against further allegations of *knowledge*. The District Court found that Napster had *actual knowledge* of copyright infringement by users as shown in a document authored by Napster co-founder Sean Parker. The Parker memo referred to "the need to remain ignorant of users' real names and IP addresses 'since [the users] were exchanging pirated music.'"³³ The District Court found additional evidence representing a mix of *actual* and *constructive* knowledge of infringement: Napster executives had recording industry experience, (Napster had claimed that its "executives [had] 'record label experience' totaling 45+ years in all"³⁴ in the hopes of gaining attention from prospective investors); Napster executives had enforced intellectual property rights in other instances ("Napster steadfastly protect[ed] its own intellectual property, including its copyrighted software – which users must agree not to infringe before downloading"³⁵); Napster executives had downloaded copyrighted songs from the system (the plaintiffs alleged that "every single Napster executive's downloads contained blatantly infringing recordings"³⁶); Napster had promoted the website with "screen shots listing infringing files;"³⁷ and "internal Napster documents reveal[ed] that even when Napster executives made a presentation using 'screenshots' of the Napster service, those screens [did] not list unknown

³² *Napster*, 239 F.3d at 1021.

²⁵ *Napster*, 114 F. Supp. 2d at 901.

³⁴ Russell J. Frackman, on behalf of Mitchell Silberbert & Knupp, LLP, and Carey R. Ramos, on behalf of Paul Weiss Rifkind Wharton & Garrison, attorneys for A&M Records et al., Joint Motion for Preliminary Injunction, A&M Records et al. v. Napster (filed June 12, 2000) at 14.

³⁵ *Id.* See also, e.g., *Castle Rock Entertainment v. Carol Publishing Group, Inc.*, 955 F. Supp. 260, 267 (S.D.N.Y. 1997).

³⁶ *Id.* at 13.

³⁷ *Napster*, 114 F. Supp. 2d at 901.

artists. They list[ed] top artists.”³⁸ On the basis of all this evidence, the District Court concluded that Napster’s executives’ actions revealed their *knowledge* of the copyright infringement that occurred by their users through the system.

Contributory Element #3: Material Contribution

Under the third element of contributory infringement, the defendant must materially contribute to the infringing activity of its users. In a classic pre-Internet example, Fonovisa, a recording company specializing in Latino and Hispanic music, sued a California swap meet for contributory infringement of copyrighted music.³⁹ Cherry Auction, the swap meet, provided the site and facilities for vendors to sell music to the public. Several of these vendors were selling pirated copies of Fonovisa’s copyrighted recordings. The Ninth Circuit found that providing the rental space and facilities for this infringement constituted material contribution, and thus Cherry Auction was liable for contributory infringement.⁴⁰

The District Court found that Napster also “materially contributed to the infringing activity [of its users] by providing support services that allowed users to conveniently locate and download copyrighted files.”⁴¹ The Napster program provided the site and facilities for users to exchange copyrighted music. Napster provided tools such as the search function, linking system, hotlist, and chat room features, which allowed users to find, copy, and distribute copyrighted music from one another. Users remained totally anonymous while using these tools, making them practically immune to the consequences of illegally exchanging copyrighted music. These features revealed that Napster materially contributed to users’ illegal activity. Without the P2P software and centralized server system provided by Napster, infringement would not have taken place in this convenient and extremely popular venue. Thus, the plaintiffs had satisfied each of the three elements needed to hold Napster accountable for contributory copyright infringement.

³⁸ *Id.* at 901.

³⁹ See *Fonovisa v. Cherry Auction*, 76 F.3d 259 (9th Cir. 1996).

⁴⁰ Cherry Auction also had *actual knowledge* of the infringing actions of its vendors because it had been notified of such by the Fresno County Sheriff as well as Fonovisa. See *id.* at 263-64.

⁴¹ Lisa Zepeda, *I. Intellectual Property: A Copyright: 1. Digital Media: d) Digital Music Distribution: A & M Records, Inc. v. Napster, Inc.*, 17 Berkeley Tech. L. J. 71 (2002).

Vicarious Copyright Infringement

In addition to the contributory infringement claim, the plaintiffs also brought a separate claim against Napster under the doctrine of *vicarious* copyright infringement. To establish *vicarious* infringement, the plaintiffs needed to prove:

- (1) A direct infringement (by Napster's users) occurred ;
- (2) The defendant (Napster) derived financial benefit from the infringing activity; and
- (3) The defendant (Napster) had the right and ability to supervise the activity of its users.

Vicarious Element #1: Third Party Infringement

Once again, in order to satisfy the first element of the vicarious infringement doctrine, the plaintiffs had to demonstrate that Napster's users were engaged in direct copyright infringement. The Court found that within the peer-to-peer file-sharing environment, at least some of the users were reproducing and distributing copyrighted files without authorization. The users' downloading and uploading activities violated the copyright owners' exclusive rights to reproduction and distribution, thereby supporting the allegation of direct infringement.

Vicarious Element #2: Financial Interest

Under the second element of vicarious infringement, the plaintiff must show that the defendant has some sort of financial incentive to allow (or ignore) the infringing activity of its users. In the *Fonovisa* case, the Cherry Auction swap meet charged its vendors a fee to rent a spot and charged its customers an entrance fee to enter the swap meet. The Ninth Circuit specifically stated that the illegal music acted as a "draw" to the paid venue. Thus, the court was satisfied that Cherry Auction had a financial interest in allowing these vendors to continue selling their popular (albeit illegal) pirated music.⁴²

The Napster Court decided that tangible profits did not need to be present to show that Napster had a financial interest in allowing infringement by its users. In the information age, advertising strategies focus on the accumulation of "eyeballs," the raw number of Internet users who are exposed

⁴² *Fonovisa*, 76 F.3d at 260-64.

to ads on websites they visit. The belief is that even though some users do not click on the banner for more information, the fact that they are constantly exposed to the visual image keeps the advertisement in mind. Exposure to ads was important for Napster because as a free service it did not collect revenue from its users. Napster yielded its income from advertisers who paid in proportion to the number of users that viewed the website and theoretically saw the advertisements. This was a financial incentive for Napster to continue to acquire new users and condone the illegal activity.

In addition, documents retrieved from Napster executives also showed the company's economic forecast. Napster's interest in increasing the user base was linked to a planned "network effect." This meant that if Napster could become indispensable to users of the system, others would want to join due to the popularity of the service. The District Court and Ninth Circuit specifically found that Napster's future revenue was directly dependent upon such increases in the user base. More and more users would be attracted to the Napster service as the "quality and quantity of available music increase[d]."⁴³ The District Court pointed out that other potential revenue sources, such as targeted emailing, advertising, and commissions from links to commercial websites, were all directly related to the size of the user-base. An increase in the quality and quantity of available music might attract investors as well.

Finally, the District Court noted that once Napster established a large enough user-base, it could have begun to charge a fee for its services. Evidence suggested that Napster planned to make the change to a fee-based service once a sufficient user base had become dependent upon it. According to the Ninth Circuit, "financial benefit exist[ed] where the availability of infringing material 'act[ed] as a 'draw' for customers."⁴⁴ The availability of infringing material attracted more users to the Napster system. Nearly 90% of the songs being shared were copyrighted recordings, a strong indicator that most of Napster's users were drawn to the system because they would be able to download copyrighted songs that they would otherwise have to buy.⁴⁵

All of these factors pointed to Napster's financial interest in the illegal activities of its users. While the company did not yield any profits from the illegal act directly, there was evidence that Napster did receive both current and prospective financial benefits from such infringing acts. Based on these

⁴³ *Napster*, 239 F.3d at 1022.

⁴⁴ *Id.*

⁴⁵ *Napster*, 114 F. Supp. 2d at 898.

assumptions, the Courts ruled that Napster had a financial interest in tolerating the infringing activity of its users.

Vicarious Element #3: Right and Ability to Supervise

The third element for vicarious infringement reviewed by the Court was the right and ability of Napster to supervise the activity in question. In prior cases such as *Fonovisa*, the existence of both a *legal right* and the *physical ability* to control users had been relevant to this aspect of the analysis. The legal right to control user activity is often found through contractual agreements, such as the contract that gave the Cherry Auction swap meet the legal authority to supervise the venue and exclude vendors who violated the law.⁴⁶ The physical ability to supervise user behavior varies by context: a "dance-hall operator" can observe whether copyrighted music is performed in the venue without authorization, while a "mere landlord" usually has no physical access to monitor what type of music a lessee plays inside a leased apartment.⁴⁷

Napster users were required to sign a terms of use agreement in order to obtain the software. The agreement stated that Napster could, at any time, terminate the account for any reason. This was viewed by the courts as evidence that Napster maintained the *legal right* to supervise the activities of its users. The user agreement stated that users should not exchange copyrighted music, but the rules against piracy were inconsistently enforced. In 1999-2000, Napster did ban some users but information soon circulated on the Internet as to how to get a new username and start trading all over again.⁴⁸ Napster took no steps to prevent the fairly simple process of working around its user agreement. The Ninth Circuit maintained that "to escape imposition of vicarious liability, the reserved right to police must [have been] exercised to its fullest extent."⁴⁹ In other words, Napster was not being penalized for having reserved the legal right to police the system. Instead, by reserving the right and then failing to use it, Napster opened itself up to potential liability as a vicarious infringer.

⁴⁶ *Fonovisa*, 76 F.3d at 260-64.

⁴⁷ *See id.* for a more detailed discussion of the "dance hall" and "landlord" line of case precedents.

⁴⁸ Frank Bourbon, *Napster Ban Work-Around*, ZDNet Music (2004), at <http://ankarino.tripod.com/frankb/frankbourbon5.html>.

⁴⁹ *Napster*, 239 F.3d at 1023.

In finding that this element of vicarious infringement had been satisfied, the District Court also implied that Napster had the *physical ability* to supervise user behavior. Unlike the District Court, however, the Ninth Circuit recognized some of the technological limits of the Napster system. Under the current architecture, Napster did not have the ability to locate the infringing material within the MP3 files themselves; Napster only read the file titles that appeared on the indices, not the content of those MP3 files. According to the Court, the file name indices were within the “premises” that Napster could police, because Napster had access to the central indexing server. However, those file names were created by individual users, with no guarantee that the names were accurate. Taking into account such limitations, the Ninth Circuit thought it more appropriate to place some of the burden on the RIAA to provide Napster a detailed list of infringing files available on the system. This bought Napster some time to implement a filter on the system, and if it made reasonable efforts to do so, vicarious liability for infringement might be avoided.

Ultimately, however, avoiding *vicarious* liability would do Napster no good if it could not avoid liability for *contributory* copyright infringement as well. Given that Napster had been caught red-handed with documents evidencing knowledge of user infringement, contributed the necessary tools for that infringement, benefited financially from the infringement, and arguably took very few steps to prevent the infringement, secondary liability was imposed. This ruling sent a signal to other P2P providers as to how they might avoid factors, such as damaging memos and centralized servers, which led to Napster's downfall.

The Aimster Case

Aimster P2P software was designed as an add-on to the popular America On-Line (AOL) Instant Messenger Program (AIM).⁵⁰ Aimster software gave AIM users peer-to-peer online file-sharing capability in addition to their existing AIM instant messaging capability. John Deep, Aimster's creator, was in no way affiliated with AOL or AIM; he simply created a technology that was compatible with their products.

⁵⁰ In re Aimster Copyright Litigation, 334 F.3d 643, 646 (7th Cir. 2003). AOL Instant Messenger is free software that was created by America Online that provides Instant Messaging service, which is the ability for users to see if friends or co-workers are connected to the Internet and exchange messages with them.

The Aimster Technology

Aimster software could be downloaded free of charge from Deep's website and could only be used in conjunction with AOL's AIM instant messaging service. The Aimster software allowed AIM users to attach and share files during the course of their online communication. Thus, AIM users were empowered to engage in the sharing of music, movies and other media while communicating online. In addition, Deep offered a service called "Club Aimster" for users who were willing to pay for access to a *top 40* downloaded list.

The Aimster software functioned like most other P2P sharing software on the Internet. In other words, it provided an index of the files that were available to download from other users.⁵¹ Aimster's servers connected to the user's computers and then created an index of the user's files in order to facilitate easy searches for those files. When a user searched for a file, Aimster's software searched this index and then connected her with other users that possessed the file. After that was done, the software began to download the file.⁵² Similar to the Napster system, these files were never stored on Aimster's servers.

Aimster only provided the facilities for exchanging the files.⁵³ As a result, Aimster attempted to absolve itself from legal liability by avoiding any knowledge of what its users were exchanging. This was done through an encryption system that made it impossible for Aimster to monitor the content or details of any exchanges.⁵⁴ Thus, Aimster differed from Napster in this regard.

If an individual wanted to use the Aimster service, she navigated to Aimster's website and then registered by designating both a username and a password. After registration, the user was able to add a list of friends (aptly named "buddies") to her list. By adding buddies, the user was able to communicate and exchange files with them through online instant messages. If a user did not designate a specific list of buddies, all users of Aimster were instantly available to provide downloads.⁵⁵ As with Napster, this wide-scale P2P sharing often included copyrighted music files, and so the recording

⁵¹ *Id.*

⁵² *Id.*

⁵³ *Id.* at 647.

⁵⁴ *Id.* at 650.

⁵⁵ *Id.* at 646.

industry filed a lawsuit, and Aimster was ultimately found liable for contributory and vicarious copyright infringement.

Contributory Element #1: Third Party Infringement

As with Napster, one of the claims raised against Aimster was contributory copyright infringement. If the three elements of contributory infringement could be proven, then Aimster could be held accountable for the infringing behavior of its users. Since users were copying and distributing protected works without authorization from the copyright owners, the first element of contributory infringement – ‘third party infringement’ – was proven.

Contributory Element #2: Knowledge

In order to protect itself from knowledge of infringement, Aimster argued that the encryption feature would encrypt the data that was being transmitted and thereby prevent Aimster from knowing what songs were being transmitted. The Seventh Circuit Court of Appeal rejected the argument that Aimster did not have knowledge of its users' activities because – according to the court – ‘willful blindness is knowledge’ of the infringement. Thus, if a person is aware that certain activities are illegal and willfully constructs his program so that he does not have full knowledge of those details, then he will *not* be absolved of liability for secondary liability. The court found that Deep (Aimster' s creator) had demonstrated, through his design of the system, a ‘guilty state of mind.’⁵⁶

Like Napster, Aimster raised a defense to knowledge of its users' infringement by citing the *Sony Betamax* case. Aimster argued that there were “substantial non-infringing uses” of its system; therefore, the court should not attribute *constructive* knowledge of infringement – rather, the court should hold out for evidence of *actual* knowledge of infringement. The Seventh Circuit took the position that even though there was the possibility that Aimster' s software could be used for legal means, the burden of proof still fell upon Aimster to demonstrate that the service actually had non-infringing uses. In other words, Aimster was required to prove that there were users on its network who used the service for legal means. Aimster lost on this element because it

⁵⁶ *Id.* at 650.

provided no evidence that ‘its service had ever been used for a non-infringing use, let alone evidence concerning the frequency of such uses.’⁵⁷

Contributory Element #3: Material Contribution

Regarding contribution to copyright infringement, the Seventh Circuit found that Aimster provided the search function and real-time index that enabled users to find the songs they shared.⁵⁸ Using these tools, users were able to easily search for files on the Aimster system. Aimster was no longer merely providing the place for infringing; it was also helping users infringe by allowing them to find files easily.

Vicarious Element #1: Third Party Infringement

The separate claim of vicarious infringement, the other classic form of secondary liability, was also raised in the *Aimster* case. Once again, in order to satisfy the first element of vicarious infringement, the Seventh Circuit found that at least some of Aimster's users were reproducing and distributing copyrighted files without authorization, thereby violating the copyright owners' exclusive rights to reproduction and distribution.

Vicarious Element #2: Financial Interest

Unlike Napster, Aimster had no advertising connected with its service and no damaging internal documents suggesting that it planned to charge a fee for the P2P aspect of its service in the future. Only the "Top 40 Download" function generated revenue for Aimster. However, the Seventh Circuit found that the free P2P service could not be separated from the fee-based part of the service, because Aimster relied on the money that was generated from those fees to finance the entire endeavor. Further, even though Aimster only listed 40 songs for download on the fee-based service, these same songs were copyrighted and were actively traded on the P2P service without authorization. As a result, the Court found that infringement was interwoven in all aspects of Aimster's service, thereby providing a financial incentive to ignore the users' illegal behavior.

⁵⁷ *Id.* at 652-53.

⁵⁸ *Id.* at 646.

Vicarious Element #3: Right and Ability to Supervise

Aimster also argued that it did not have the ability to supervise its users' behavior because the software encrypted all transactions before sending them over the Internet. The Court, in a somewhat circular manner, reasoned that willful ignorance was no excuse for the inability to identify (and thereby physically block) illegal behavior. Although this may sound more like a discussion of the *knowledge* element of *contributory* infringement, the Seventh Circuit used similar reasoning to determine that Aimster "could have" given itself the power to supervise the use of its system. This failure to police the system was not enough, in this Court's view, to insulate Aimster from *vicarious* liability for the users' infringement.

The Grokster Case

In the midst of what might have appeared as some internal inconsistencies in the Napster and Aimster analyses, the Ninth Circuit was soon faced with another P2P file-sharing case (which would eventually make its way to the U.S. Supreme Court as well). The 'Grokster' P2P file-sharing network gained increased popularity once Napster found itself in legal trouble. In many ways, the creators of the Grokster system were able to take advantage of lessons learned from the Napster litigation, thereby dodging liability for secondary infringement by providing a more decentralized P2P network. A broad group of music and film industry studios, among other copyright owners, hoped to convince the courts that this technological difference was *not* sufficient to insulate Grokster from legal liability.

The Grokster Technology

The primary difference between Grokster and Napster (or Aimster) was that Grokster lacked a central server. In other words, Grokster's software did not require a central server to keep an index of files nor did it need a central server to serve as a hub for file sharing. Instead, Grokster used a system of 'supernodes' to keep track of files on the network. A supernode can be defined as a set of computers that work together to maintain an index of files. In essence, the computers that were keeping track of files on the Grokster network were the users' computers. Moreover, if any of the computers that were acting as a part of the supernode shut down or were removed from the network, then the responsibilities of maintaining the index automatically shifted to other computers on the network. At any given time, there could be millions of

computers that were sharing files while a few hundred computers acted as the network's supernodes. A user's computer could be part of a supernode on a given day without her ever realizing it.

In order for a user to log onto Grokster's network, she must first download and install the software. Next, the user created a folder on her computer where files to be shared with the rest of the network were stored. After a few more adjustments, the user was able to download and upload files by searching the index.⁵⁹ Through the network, a user was able to download almost any form of data ranging from text files to movies files, both legal and illegal.

Grokster did not require the users to complete a formal registration process. The network merely kept track of users via their Internet Protocol Address.⁶⁰ With this the user's anonymity and privacy were assured. Grokster was not able to control what or when a user downloaded. No data was transferred to Grokster's servers. The only time there was any interaction between Grokster and the user was during the initial download of the software, limited technical support, and whenever the user visited Grokster's website. Grokster never came into contact with any user information, did not know the contents of what the users were sharing, and did not have direct access to the file-sharing index. Grokster was unable to control how the network was actually being used because the software was designed to be as organic and formless as possible.

This was the key technological difference between Grokster and its predecessors. With the exception of technical support and possible software upgrades, Grokster's involvement in the P2P process stopped after the user downloaded and installed the software. While the other services (such as Napster and Aimster) had continued to operate in order to maintain the P2P file index, Grokster's software could operate indefinitely, without any central

⁵⁹ For the purposes of helping users find files more easily, the creators of Grokster included a search function in their software. When a user wanted a file, they were able to run a search on the supernode's index. By typing in the name of the specific file, they were able to easily find a copy of the file on the network. For example, if a user wanted to find a certain song, the user only needed to search for the name or author of the song and the query would result in a list of potential matches. After doing this, all the user had to do was click on the file to download it from other users.

⁶⁰ An Internet Protocol Address (or IP Address) is a unique number that is assigned to any computer that is logged on to the Internet. They can be both dynamic (where the address changes often) or static (where the address never changes).

control, as long as members of the public continued using the software. Even if Grokster was shut down, as long as users still used the software, the network would continue to exist. The notion of secondary liability for such a limited player in the P2P process (i.e., the mere provider of computer software that might – or might not – be abused) made the legal analysis more complicated than ever before.

Contributory Element #1: Third Party Infringement

As with Napster and Aimster, one of the claims raised against Grokster was contributory copyright infringement. When dealing with the first element of contributory infringement, the District Court examined the behavior of Grokster's users. Like the previous cases, with P2P file-sharing at least some of the users were assumed to be reproducing and distributing copyrighted files without authorization. The users' downloading and uploading activities violated the copyright owners' exclusive rights to reproduction and distribution respectively. Therefore, the first element of contributory infringement – 'third party infringement' – could be proven. If the remaining two elements of contributory infringement could be proven, then Grokster could be held legally accountable for its users' behavior.

Contributory Element #2: Knowledge

The District Court found the creators of the software *constructively* knew that Grokster could be used for infringing purposes.⁶¹ However, Grokster also proved that its software had significant non-infringing uses. Like Napster (and unlike Aimster), Grokster provided examples of copyright owners who allowed their work to be shared over the system. One example was the band Wilco, whose record company would not release their album. Wilco allowed the distribution of their album over Grokster's network. As a result, Wilco became quite a bit more popular and their record company offered them another record contract. There were thousands of other groups who also benefited as result of Grokster, which was evidence that Grokster was capable of substantial non-infringing use as applied in the *Sony-Betamax* precedent.

Because Grokster was capable of substantial non-infringing use, the plaintiffs were left with the burden of proving that Grokster had *actual* knowledge of infringement. As stated by the Court, there must have been

⁶¹ Metro-Goldwyn-Mayer Studios, Inc., et al. v. Grokster, Ltd., et al., 259 F.Supp.2d 1029, 1162 (C.D. Cal. 2003).

evidence that Grokster had "reasonable knowledge of specific infringement"⁶² and "failed to act upon that information."⁶³ Like Aimster (and unlike Napster), no such "smoking gun" evidence of actual infringement was presented. In addition to the lack of documentary evidence, the unique nature of Grokster's technology made it difficult to point toward knowledge of specific instances of infringement. Grokster did not maintain an index of shared files; the index was actually maintained by the users (supernodes) and because of that aspect of the technology, Grokster's knowledge of infringement was not enough to satisfy the legal standard.

Contributory Element #3: Material Contribution

The District Court also found that Grokster did not materially contribute to the infringement of its users. Unlike Napster and Aimster, Grokster did not provide the storage place or the centralized index for the users and was unable to suspend user accounts. The software was designed in such a way that the users of the software were the ones that maintained the massive index of files. Additionally, Grokster did not store any of the copyrighted files on their centralized servers. All of the storage space for the P2P file sharing from the users. The users themselves created the network of supernodes and provided the storage space for the allegedly infringing materials.⁶⁴ Once users were in possession of the software, Grokster could cease to exist and the P2P file sharing would still continue uninterrupted.

If Grokster provided the site and facilities, or if Grokster stored files and failed to delete the listings, then this could have been considered a material contribution to user infringement. Without such contribution, however, Grokster merely supplied a software program with legal (and illegal) potential uses. The Court agreed that Grokster's P2P file-sharing technology was more than a mere tool to facilitate copyright infringement; instead, it reduced distribution costs of public domain⁶⁵ art and speech. To treat the distribution of such software as 'material contribution to copyright infringement' could start a slippery slope that would soon stifle many forms of publicly valuable

⁶² *Id.* at 1035.

⁶³ *Id.* at 1036 (citing *Napster*, 239 F.3d at 1021).

⁶⁴ *Grokster*, 259 F.Supp.2d. at 1037.

⁶⁵ Artistic works enter the 'public domain' when their copyright term expires. The term 'public domain' is also used loosely to describe works that do not qualify for copyright protection for various other reasons.

technological development. The Ninth Circuit agreed with this reasoning that Grokster could not be held liable for contributory infringement.

Vicarious Element #1: Third Party Infringement

Again, as with Napster and Aimster, the other claim raised against Grokster was vicarious copyright infringement. Since users were copying and distributing at least some protected works without authorization by the copyright owners, the first element of vicarious infringement – ‘third party infringement’ – could be proven. Thus, if the remaining two elements of contributory infringement – ‘Grokster’s financial incentive’ and ‘Grokster’s right and ability to supervise’ the users’ behavior – could be proven, then Grokster could be held legally accountable for vicarious infringement.

Vicarious Element #2: Financial Interest

The element of direct financial benefit was undisputed. Like Napster (and unlike Aimster), Grokster sold access to advertising windows on its software interface. There were banners on Grokster’s software screen that displayed advertisements at all times. The amount of money Grokster made depended on its user base, because the more users, the more people advertisers reached, and in return the more money the advertisers were willing to pay. The greater number of direct infringers on the Grokster network financially benefited Grokster. This was evidence that Grokster did have a financial incentive in promoting its software and increasing its user base, even if some of those users were copyright infringers.

Vicarious Element #3: Right and Ability to Supervise

The Ninth Circuit found, however, that Grokster did *not* have the right and ability to supervise the infringing behavior of its users. Grokster did not display any ability to block individual users and lacked a registration and log-in process. There was no communication between Grokster and users during a search for files because no information passed through Grokster. This distinguished Grokster from the Napster system, which included an ‘integrated service’⁶⁶ that monitored and controlled user information. The right and ability to supervise seen in past vicarious liability cases such as Napster and Aimster (or even Fonovisa) did not exist for Grokster.

⁶⁶ *Id.* at 1045.

The plaintiffs argued that Grokster' s capacity to update its software was evidence of its right and ability to supervise use of the software. Alternatively they argued that Grokster was turning a "blind eye" to the infringement of their users. The Ninth Circuit was unpersuaded by either of these arguments. This created a possible split from the Seventh Circuit' s interest in the "blind eye" theory of liability. Ultimately, the Ninth Circuit found that Grokster' s specific technology was shielded from vicarious liability as well as contributory liability. The ruling prompted the plaintiffs to appeal the case to the U.S. Supreme Court.⁶⁷ The Grokster Plaintiffs, along with the content industry in general, intended to use the case as a platform to argue for an Internet-era interpretation of secondary copyright infringement liability that could shut down even a fully decentralized system such as Grokster.

DISCUSSION: SHOULD THE COURT STRETCH COPYRIGHT LAW
TO PROTECT THE RECORDING STUDIOS?

The same essential policy question underlies the three cases examined in this article. That question is: how much responsibility should a software provider bear for potential (illegal) uses of its product by consumers? Extreme responses to this question would lead to undesirable results. For example, on the one hand, if the software provider bears *full responsibility*, then even the architects of the Internet could be found liable for secondary copyright infringement. On the other hand, however, if the provider bears *no responsibility*, then those who blatantly profit from promoting copyright infringement would face no legal repercussions. Thus, a balance must be struck somewhere between these two positions.

The Constitution does not speak directly to computer software or P2P file sharing. Certainly, the Founders never envisioned this specific form of technology. Instead, the Constitution speaks of the underlying policy balance in broad terms. In the somewhat analogous case of video tape recorders, the Supreme Court has elaborated on this delicate balance:

The limited scope of the copyright holder's statutory monopoly ... reflects a balance of competing claims upon the public interest: Creative work is to be encouraged and rewarded, but private motivation must ultimately serve the cause of

⁶⁷ This article predates a decision by the Supreme Court in the *Grokster* case.

**University of California
Irvine
Law Forum Journal**

Vol. 3

Fall 2005

promoting broad public availability of literature, music, and the other arts. ... [T]he ultimate aim is, by this incentive, to stimulate artistic creativity for the general public good. ... When technological change has rendered its literal terms ambiguous, the Copyright Act must be construed in light of this basic purpose.⁶⁸

When it comes to P2P technology, Congress (by way of the Copyright Act) has provided no specific guidance. Even the contours of the legal standards for secondary copyright infringement are a product of judicial decision-making rather than specific sections of the Copyright Act.

With the upcoming *Grokster* appeal, the Supreme Court will once again find itself in the position of striking the appropriate balance between the copyright incentive to produce and the countervailing concerns over government-sanctioned monopolies on creative expression. As the Supreme Court reaches this point, the parties to this case and Internet users at large are waiting with anticipation. Will the Court construe the current legal standards for secondary infringement liberally, thereby aiding the content owners such as the Recording Studios in their efforts to curtail P2P file sharing? Alternatively, will the Court construe the current legal standards for secondary infringement narrowly, thereby leaving the door open for the growth of P2P technology while simultaneously leaving the content owners searching for other methods to control widespread copyright infringement?

The following sections provide a brief summary of the public policy arguments that have been raised in association with this dispute. These arguments have been organized along the same lines as the “four forces for constraining behavior” posited by constitutional law scholar Lawrence Lessig.⁶⁹ Although detailed discussion of each argument is beyond the scope of this article, this brief survey helps to demonstrate that the policy arguments surrounding copyright control and emerging technology can become every bit as complex as the legal arguments.

⁶⁸ *Sony Betamax*, 464 U.S. at 431-32 (quoting *Fox film Corp. v. Doyal*, 286 U.S. 123, 127; *Twentieth Century Music Corp. v. Aiken*, 422 U.S. 151, 156 (1975)).

⁶⁹ See, e.g., Lawrence Lessig, *Code and Other Laws of Cyberspace* 199 (Basic Books) (1991). Lessig offers a graphic model and discussion of the four forces that can constrain behavior, either directly or by operating indirectly upon one another: law, markets, norms and architecture (i.e., physical capabilities and limitations).

The Force of Law

The previous sections of this article demonstrate the challenges in applying secondary copyright law to a decentralized P2P system like *Grokster*. Even the ruling against a centralized P2P system like *Napster* raises cause for concern. Complexities within the software and the system architecture make it difficult for the P2P provider to truly “know” whether specific users are infringing copyrights. In addition, “supervising” such P2P activity by pseudonymous Internet users provides an additional layer of technological challenges for the P2P operator. Some providers such as John Deep (*Aimster*) might go out of their way to avoid the ability to track or supervise user activity by encrypting their own technology. Attitudes differ as to whether this should make someone like Deep more accountable to copyright owners than the developers of the video tape recorders at issue in the *Sony Betamax* case.

The real danger here: if copyright law is stretched in order to encompass developers such as Deep in its web of secondary liability, how many other legitimate developers will be deterred from providing new technology for fear that they will be sued as well? Even if such developers could mount a “substantial non-infringing uses” defense, why invest the time and money to develop new technology when an expensive legal battle looms ahead?⁷⁰ Merely educating a court on the technological details relevant in this fact-specific area of the law would be quite a burden for a would-be inventor of new technology.

Law as a Restraint on Architecture

An affirmative legal duty for a P2P provider to monitor and supervise the content of files traded by its users creates an unreasonable architectural burden on society as well. At times, networks such as *Napster* and *Aimster* had millions of users. Although the network providers might have hoped to obtain some profit from their systems, they certainly did not set up their systems in a manner that would be economically viable if a huge staff of “network police”

⁷⁰ Recall that the *Aimster* Court went so far as to require the defendant (*Aimster*) to collect actual evidence of “substantial” non-infringing uses for the software, rather than putting the plaintiffs to the burden of proving that substantially all uses of the software did infringe copyrights. In any event, the cost of defending any legal action can be a strong deterrent; in a complex area of the law such as this, rulings in favor of a defendant are not likely to come cheaply or quickly.

were to be employed. Thus, a strict view of the secondary liability standards could make any further development of new distribution methods impractical.

The Recording Studios would not be disappointed to see the energy behind these new forms of content-sharing architecture come to an end. It is the very architecture of new technologies (digital media and Internet connections) that cost the Recording Studios the level of “content control” they had previously enjoyed in the world of radio airwaves and analog cassette recorders. This resistance to architectural change prompted the Studios to seek legal assistance in fighting against user-based control of new technologies.

Rather than assisting the Studios in their goal, the courts would be wise to continue the long-standing practice of calling for more specific congressional guidance. The decision to use the force of law to restrain the growth of technology should be deferred to a democratically accountable policy-making body that is fully equipped to invite broad participation in examining the issue from multiple perspectives.

Market Impact

Preserving the “status quo” within the music industry by giving the Studios more legal power to block P2P file sharing would have serious impact in the music market as well. In an unrestricted market, economic factors such as supply and demand often influence business models and pricing decisions. Once a government-sanctioned monopoly is introduced into the mix, the monopoly holder has less incentive to price competitively or to develop innovative products and distribution methods. Evidence collected throughout the course of these P2P lawsuits suggests that a substantial number of music consumers believe that recorded music is currently over-priced and they would like to take advantage of digital methods for receiving their music.

The *Napster* system and its progeny helped the Studios to see that digital downloads of recorded music should be offered sooner rather than later. Controlled methods of digital distribution are gaining more popularity every day. Even the *Napster* website now offers subscription-based, authorized music downloads for a fee. Some copyright owners may still rue the day that music was released to the public in digital format, which can be copied and traded with such ease; however, it does not appear that the major copyright owners have any plans to try putting that genie back into the bottle.

On the other hand, “unrestrained market” proponents still argue that the courts should encourage copyright owners to seek innovative ways to add value to their product rather than more effective ways to lock it up from a legal

perspective. In other words, if music consumers don't currently value music CDs enough to purchase them when an alternative is provided, then perhaps the Studios should seek ways to make those CDs more valuable than free downloads. This may sound difficult, but in fact, it simply requires thinking outside the long-standing "box." For instance, the music industry can learn from recent movie theater promotions that included a free "trading card" for all those who purchased a movie ticket. Because the trading card was valued by the target consumers of the movie in question (in this case, the youth market⁷¹), the trading card promotion stimulated movie ticket sales at such a rate that many theaters ran out of trading cards long before the promotion ended. This example represents only one of a myriad of creative cross-promotional packages that could be offered to stimulate the purchase of actual music CDs.

Normative Backlash

The final force for consideration in Lessig's model is the power of social norms. Our history contains examples where the force of law has been used to "hedge" social norms in a certain direction: consider racial desegregation of the public schools. Numerous sociologists and historians have argued that in a large and diverse society, such as the United States, social norms don't wield nearly as much power as formal law. However, social norms cannot be completely discounted in any society.

As the evidence collected in the P2P cases demonstrated, a growing contingent of Americans of all ages began to adopt the attitude that recorded music should be "free." Recording Studios have been viewed as the big bad bullies who stand in the way of this trend. For every artist who publicly appeals to the public not to "steal" music, another artist has declared public support for uninhibited file sharing. Whether P2P users realized that their behavior was illegal or not, a significant number of them certainly came to believe that their behavior was socially acceptable.

Why should the courts, Congress, or even the Recording Studios, care about social norms? From one perspective, a norm of lawlessness or disrespect for intellectual property rights should not be ignored. The longer a social norm is shared by a wide group of citizens, the more momentum it can gain and the

⁷¹ Trading cards associated with popular animated programs such as "Pokemon" and "Yugioh" have been extremely popular with the youth market. In fact, the cards are so popular that an after-market has emerged and some parents are known to pay more than 100 times the original sales price to acquire a child's favorite card.

more difficult it will be to combat that norm later. On the other hand, directly attacking a popular norm through law can lead to the creation of a counter-culture: consider the existence of a “black market” for everything from prostitution to illegal drugs. Even the pirated music CDs found at the Cherry Auction Swap Meet in the *Fonovisa* case were purchased by many consumers with the full expectation that those cheap recordings were illegal.

A “black market” for free music downloads will be difficult to prevent, given that so many computer servers are physically located in remote enclaves outside the United States. The growth of a counter-culture seeking illegal music downloads could not only detract from any new products or business models offered by the copyright owners, it could also undermine the very concept of “legal rules” for a significant number of P2P users. The Internet already allows for anonymity; given the incentive, P2P users might become even more comfortable simply hiding their online behavior. Perhaps even the Supreme Court took this possibility of a normative backlash into account when resisting the call to outlaw video tape recorders in the *Sony Betamax* case.

CONCLUSION

This article has provided a detailed explanation of the legal standards applicable to claims for secondary copyright infringement. This discussion illustrates that P2P technology (arguably) skirts loosely around the type of *knowledge* or *supervisory control* that might be expected when holding a software provider accountable for the infringement of its users. The legal analysis is subjective enough that the Supreme Court might rule that even *Grokster*, the most decentralized P2P system in the group, is legally accountable for its users’ behavior. On the other hand, the Court may find that the *Grokster* system defies application of the current legal standard.

Rather than using the law to restrain technological development (thereby ignoring the potential for normative or market-based harm), the content owners might find a smoother path to protection of their interests by using architecture to their benefit. Copyright owners have the power to alter the architecture of their products and their distribution methods in light of evolving consumer preferences. They also have the potential for developing stronger architectural barriers (such as encrypted products and smart playback devices) to protect their products from copyright infringement -- without the assistance of the legal system. In fact, the Recording Studios have already

undertaken efforts to do this, demonstrating that they may be quite conscious of Lessig's differing forces for constraining undesirable behavior.

The last word of caution that these authors can offer is this: copyright owners should not overlook the potential strength of norms such as "free sharing of music." Attempting to attack such a norm through architecture can lead to consumer frustration (as in the case of CDs that don't operate properly in preexisting music players). Of even greater concern, attacking a norm with the force of law can lead to a "black market" counter-culture that brings with it numerous pitfalls for society. Only by appreciating the underlying attitudes that fuel a social norm can the content owners seek to attack that norm *directly* - through education, through the dissemination of information about the harms of taking music without compensation to the creator, and perhaps through some market-based concessions in the form of innovative product improvements. Fully appreciating the interplay between law and these other social forces could be more valuable to content owners than any favorable decision in court. Throughout all of this one thing is certain: the digital revolution -- including new technologies such as peer-to-peer file sharing -- is here to stay.

EDITORS' NOTE:

In June of 2005 the Supreme Court ruled, unanimously, that Grokster was liable for secondary copyright infringement based upon the activities of its P2P users.⁷² Rather than construing the traditional legal standards more liberally than the Court of Appeal, the Supreme Court surprised some observers by crafting what might be called a "third form" of secondary copyright infringement -- referred to by some commentators as "inducement infringement." Other commentators have simply described this as a more liberal approach to contributory copyright infringement; the new approach does not delve as deeply into the "knowledge" inquiry or "substantial non-infringing uses" defense, if the plaintiff can show that the defendant "actively induced" the third-party infringement.

The Court found that Grokster "induced" copyright infringement by holding itself out to Napster's former network of copyright infringers as

⁷² Metro-Goldwyn-Mayer Studios, Inc. v. Grokster, Ltd., 125 S.Ct. 2764 (2005).

University of California
Irvine
Law Forum Journal

Vol. 3

Fall 2005

“Napster’s successor” and by its failure to develop any sort of filtering tools to reduce the amount of infringement among these users. The Court declined, however, to state that all technology or service providers have an affirmative duty to minimize the use of their products or services for infringing purposes. The decision leaves a great deal of room for interpretation by the lower courts, and provides little reassurance to technology developers who fear the burden of potential lawsuits.

The authors of this article will likely be disappointed to see that the Court has skirted their arguments as to the shortcomings of current legal standards. By “stretching” the legal standard the Court has given the content owners a great deal of ammunition to use law as a force to constrain technological development. Thus, Congress has less incentive to examine the competing interests more carefully from a policy perspective, and the content owners have no particular incentive to explore innovative new business models. Perhaps as news of the Supreme Court’s ruling spreads, P2P users will accept the notion that their behavior is illegal and stop trading copyrighted files without permission. On the other hand, the potential for the normative resistance described in this article is still present. For the sake of the perceived legitimacy of the legal system, we can only hope that the authors’ fears about a normative backlash will not be realized as well.