NEW YORK LAW SCHOOL

NYLS Law Review

Volume 46
Issue 1 *Judge Jon. O. Newman: A Symposium Celebrating his Thirty Years on the Federal Bench*

Article 10

January 2003

BEYOND NAPSTER, BEYOND THE UNITED STATES: THE TECHNOLOGICAL AND INTERNATIONAL LEGAL BARRIERS TO ON-LINE COPYRIGHT ENFORCEMENT

Jeffrey L. Dodes

BEYOND NAPSTER, BEYOND THE UNITED STATES: THE TECHNOLOGICAL AND INTERNATIONAL LEGAL BARRIERS TO ON-LINE COPYRIGHT ENFORCEMENT

I. INTRODUCTION

Courts in the United States and throughout the world are faced with great challenges in adjudicating legal conflicts created by the rapid development of digital technologies. The proliferation of new technologies that allow for fast, reliable and widespread transmission of digital files has recently created a swell of litigation and media coverage throughout the world. Copyright law, particularly in the area of music, is at the forefront of these latest developments due to the rapid rise of Napster, an internet file sharing service that allows for easy transmission of digital files directly from one computer user to another without payment.[1] In just eighteen months, Napster developed from a college campus based following of thousands, to the fastest growing home software application ever.[2] The renegade service became a worldwide phenomenon with 65 million software downloads and 16.9 million unique users as of February 2001.[3]

Napster's rapid rise in popularity raised the concerns of the Recording Industry Association of America ("RIAA") which filed a lawsuit against Napster on December 6, 1999. The RIAA alleged that Napster

1. There have been many developments with Napster, the corporation, and Napster the software application since this note was finalized. The service voluntarily shut down in July 2001 with the hopes of re-launching before the end of September 2001. As of January 2002, the service was still not available to the general public, but a "beta" version of new Napster software that is designed not to infringe copyrights was in testing with a limited number of consumers. For the latest developments and more detailed information on Napster *see* http://www.napster.com.

2. Media Metrix Press Release: Napster Software-Application Usage Soars 500 Percent To Nearly Seven Million U.S. Home Users, According To Media Metrix (Oct. 5, 2000), *available at* http://us.mediametrix.com/press/releases/20001005.jsp (last visited Jan. 29, 2001).

3. Media Metrix Press Release: Jupiter Media Metrix Announces U.S. Top 50 Web And Digital Media Properties For February 2001, Napster now is the 13th most visited property with 16.9 million unique visitors (Mar. 13, 2001), *available at* http://us.mediametrix.com/press/releases/20010313.jsp (last visited Apr. 15, 2001). By the time the service shut down in July 2001, Napster software was downloaded 80 million times.

is "operating, a haven for music piracy on an unprecedented scale"[4] and sued the Internet service for contributory and vicarious copyright infringement. In *A & M Records, Inc. v. Napster, Inc.*,[5] the district court granted the RIAA a preliminary injunction after finding that Napster would very likely be found liable for facilitating copyright infringement when a full trial is eventually held. Two days later on July 28, 2000, a panel of judges for the U.S. Court of Appeals for the Ninth Circuit reviewed the order and stayed the injunction until further hearings were held.[6]

Seven months later, on February 12, 2001, the Court of Appeals issued its opinion in *A & M Records, Inc. v. Napster, Inc.* .[7] The court upheld-in-part the district court's preliminary injunction because the RIAA had substantially prevailed on appeal, and reversed-in-part remanding for modification as to Napster's liability for contributory copyright infringement. Although the district court's injunction was not affirmed outright, essentially the RIAA won the appeal because the Court of Appeals agreed with the district court's finding of contributory and vicarious copyright infringement and rejected all of Napster's defense arguments. The court determined that the original injunction as constructed by the district court was too broad, however, and on remand placed the burden on the plaintiffs to notify Napster of the specific infringing files in question. On March 5th, the district court redrafted the injunction to conform with the Court of Appeals opinion.[8] Based on the order, once Napster received a list of copyrighted works owned by the plaintiffs, it was to block transmission and/or remove all complementary search ability for the named files on its system within three days.[9]

This decision is a clear victory for the U.S. music industry and will have considerable impact on the legal business models[10] that develop

4. RIAA Press Release: Recording Industry Sues Napster for Copyright Infringement (Dec. 7, 1999), *available at* http://www.riaa.com/PR_Story.cfm?id=70 (last visited Jan. 29, 2001).

5. 114 F. Supp. 2d 896 (N.D.Cal. 2000).

6. *See* A&M Records, Inc. v. Napster, Inc., 2000 WL 1182467 (9th Cir. Jul. 28, 2000).

7. 239 F.3d 1004 (9th Cir. 2001).

8. *See* A&M Records, Inc. v. Napster, Inc., 2001 U.S. Dist. LEXIS 2186 (N.D.Cal. Mar. 5, 2001).

9. *See id.*

10. The RIAA believes that "what Napster is doing threatens legitimate e-commerce models and is legally and morally wrong." *See* RIAA Press Release: Music Industry

for the digital distribution of music and other copyrighted material over the Internet. This begs the question, however, whether the legal precedent created by the RIAA's victory will prevent similar copyright infringement by Internet services in other countries. There are already international treaties in place that help protect copyright holders from infringement outside the United States,[11] but ultimately each individual country's copyright laws are applied to determine infringement in that country. This creates possible problems for on-line copyright enforcement when the infringing service is based outside of the United States.

In addition to the legal difficulties of enforcing a U.S. based copyright infringement judgement abroad, there are significant technological and ideological barriers to enforcement as well. Even with a judgement in their favor, a plaintiff may have no remedy because based on new file sharing systems, the infringement may be nearly impossible to prevent technologically. The developers of some of these systems hold radical views on copyright and scoff at the idea of intellectual property. Some have even gone so far as to design their technologies to fall within gaps in current copyright law. These technologies are so well developed and distributed that offensive technological measures may be the only method of stopping them. Yet these measures create various public relations and privacy law problems that make them potentially undesirable.

While courts of law and international treaties will continue to be significant factors in the prevention of on-line copyright infringement, they will not be able to solve the problem alone. A true solution also requires new business models and strengthening current copyright law. The current law provides the standards for determining copyright infringement, but stricter infringement standards are necessary to deter the development and deployment of illegal file sharing services. The music industry must also develop creative alternatives to copyright infringement in the short term, as well as workable digital distribution

Files Motion for Preliminary Injunction Against Napster (June 12, 2000), *available at* http://www.riaa.com/PR_Story.cfm?id=284. (last visited Jan. 29, 2001).

11. See The Agreement on Trade-Related Aspects of Intellectual Property Rights (1994), *available at* http://www.wto.org/english/tratop_e/trips_e/t_agm0_e.htm (last visited Jan. 28, 2001); WIPO Copyright Treaty (1996), *available at* http://www.wipo.org/treaties/ip/copyright/copyright.html (last visited Jan. 28, 2001); WIPO Performances and Phonograms Treaty (1996), *available at* http://www.wipo.org/treaties/ip/performances/performances.html (last visited Jan. 28, 2001).

models in the long term or they risk continued widespread infringement of their copyrights.

Part II A of this note explores American copyright law as well as international treaties that may apply to a case of copyright infringement. To place these issues in the proper context, Part II B includes a brief explanation of the current digital technologies that are making traditional legal principles more difficult than ever to apply. Part II C looks at Napster's defense arguments and their treatment by the Court of Appeals. Part III A goes on to analyze a hypothetical scenario where Napster is enjoined in the United States, but moves to another country to rebuild its service and continues contributing to the illegal copying and distribution of music files. Part III B discusses the emerging infringing technologies, their ideologue developers and the problems they present for copyright enforcement. Part IV makes some recommendations for a solution to widespread digital copyright infringement of music on the Internet. Part V concludes that current copyright law is central to the solution of rampant on-line copyright infringement, but that it cannot solve the problem on its own. The solution requires a strengthening and broadening of current copyright law, development of technological measures to counteract the newest insidious file sharing technologies and new creative business models to offer legal digital music to the public.

II A. General Copyright Background

The Copyright Act, Title 17 of the United States Code, grants the exclusive rights of creators to their creative expression.[12] The Act grants a number of exclusive rights, including the right of reproduction, distribution, adaptation, public display and public performance of an owner's works.[13] It extends only to original expressions and does not protect ideas, systems, procedures, concepts and factual information or protect pre-existing ideas in the copyrighted work.[14] Section 102 of the Copyright Act extends this property right directly to musical compositions and Section 114 grants copyrights in sound recordings.[15]

In granting and enforcing these rights, Congress and the courts must balance the law's objectives of promoting widespread distribution of original creative works, while providing incentives to authors and

12. *See generally* 17 U.S.C.A. §106; *see also* U.S. Const., art. I, § 8, cl. 8.
13. *See* 17 U.S.C.A. §106.
14. *See generally* 1 Nimmer On Copyright Ch. 2 (2000).
15. *See* 17 U.S.C.A. §102; 17 U.S.C.A. §114.

owners to create such works.[16] In keeping with this "balancing act" Congress has amended Title 17 many times since it was enacted to keep pace with technological advances. Recent amendments include the Audio Home Recording Act and the Digital Millenium Copyright Act.[17] Current advances in technology continue to put pressure on this balance by allowing works to be easily copied without permission from copyright owners and thereby requiring yet another reevaluation of copyright law.

Changes in the Copyright Act that were triggered by the Internet started to appear in 1995 when the Digital Performance Right in Sound Recordings Act ("DPRSA")[18] was enacted. This law provides limited[19] copyright protection to public performance rights in sound recordings and grants royalties to copyright owners for the digital performance of their works. In October 1998, Congress enacted The Digital Millennium Copyright Act (DMCA).[20] Upon signing the DMCA into law, President Clinton declared that the goal of the new act was to respond to "fundamental changes in copyright commerce caused by the Internet" and to "protect from digital piracy the copyright industries that comprise the leading export of the United States."[21]

16. *See* David N. Weiskopf, *The Risks of Copyright Infringement on the Internet: A Practitioner's Guide*, 33 U.S.F. L. REV. 1, at 9-10. (1998).

17. *See Statutory Enactments Contained in Title 17 of the United States Code*, *available at* http://www.loc.gov/copyright/title17/circ92.html#preface (last visited Jan. 28, 2001). A partial list includes: Pub. L. No. 96-517, 94 Stat. 3015, 3028 (amending §101 and §117, Title 17, United States Code, regarding computer programs), enacted December 12, 1980, Pub. L. No. 100-617, 102 Stat. 3194 (extending for an additional eight-year period certain provisions of Title 17, United States Code, relating to the rental of sound recordings and for other purposes), enacted November 5, 1988, Audio Home Recording Act of 1992, Pub. L. No. 102-563, 106 Stat. 4237 (amending Title 17 of the United States Code by adding a new chapter 10), enacted October 28, 1992, No Electronic Theft (NET) Act, Pub. L. No. 105-147, 111 Stat. 2678, enacted December 16, 1997, Digital Millennium Copyright Act, Pub. L. No. 105-304, 112 Stat. 2860, 2887 (Title IV amending §108, §112, §114, chapter 7 and chapter 8, Title 17, United States Code), enacted October 28, 1998.

18. *See* Digital Performance Right in Sound Recordings Act, Pub. L. No. 104-39, 109 Stat. 336 (1995) (codified at 17 U.S.C. 106(6), 114).

19. The public performance right granted by the DPRSA extends to owners of sound recordings when the recordings are digitally performed by either a subscription transmission or a transmission by an interactive service, but not by transmission via a non-subscription broadcast service.

20. *See* The Digital Millennium Copyright Act, 17 U.S.C. §1201 (1998).

21. *See* Jon A. Baumgarten et al., *New Year Details Ownership Rights on the Internet: The Year-Old Digital Millennium Copyright Act Leaves Little Room for Judicial Interpretation*,

Title I of the DMCA adds a new Chapter 12 to Title 17 of the United States Code that prohibits the circumvention of technological measures that control access to a copyrighted digital work.[22] The practical effect is to prevent circumvention of protective measures, such as the digital rights management or digital watermarking technologies discussed infra, but the provision is also being used by new file sharing technologies to insulate themselves from certain theories of copyright infringement.[23]

Title II of the DMCA includes the Online Copyright Infringement Liability Limitation Act.[24] Section 512 limits or negates the liability of certain entities in the chain of technologies involved in copyright infringement on the Internet.[25] Essentially, Title II of the DMCA forces copyright owners to target the actual infringers, those individuals who upload songs without permission, instead of simply the Internet Service Provider (ISP).[26] In order to qualify for a "safe harbor," upon proper notice, the ISPs must remove infringing material from its service, instead of ignoring its presence. In doing so, the DMCA punishes the specific user who is responsible for online music infringements instead of the ISP in certain circumstances. At the same time it creates a potential loophole for ISP's to claim no responsibility for the infringing actions of their users without prior notice, even if they know that infringement may be taking place. It is exactly this loophole that Napster used unsuccessfully as one if its central defense arguments.[27]

NAT'L L.J. (Oct. 25, 1999) *available at* http://test01.ljextra.com/na.archive.html/99/10/1999_1018_80.html (last visited Jan. 28, 2001).

22. *See* 17 U.S.C. §1201-05 (1999).

23. *See infra* note 164.

24. *See* 17 U.S.C. §512 (1998).

25. This portion of the DMCA is the "safe harbor" provision that exempts service providers from liability for unauthorized copyright infringement. To be eligible, the service provider must not know of or initiate the infringement, must not derive any financial benefit from the unauthorized use and must take certain actions to prevent infringement on their servers when notified of such activity.

26. An Internet Service Provider or "ISP" as it is commonly referred to is any provider of access to the Internet and the World Wide Web. This can be a service provided for private individuals or business customers. The ISP generally has a large network of computer servers that are connected to the backbone of the internet. Metaphorically, an ISP is an "on-ramp" to the on-line super-highway. In most cases, ISPs provide extra services such as Email and News Groups and sometimes their own content as well. ISPs provide connectivity to their customers through dial-up connections using the customer's own computer, modem and phone line or over dedicated lines that are established by local telephone companies.

27. *See* discussion of Napster's defense at 22,23.

Technological advances, coupled with the fact that the Internet is an international medium, have also lead to the enactment of laws and treaties that protect copyrights outside of the United States. Since copyright laws are territorial in nature, copyrights protected in the U.S. are not necessarily protected under the copyright law of another country, unless certain conditions are satisfied.[28] If a particular copyrighted work is protected under the laws in its country of origin, it then must be determined whether the material is eligible for protection in another country.[29] If the law of another country is not clear whether the copyright is protected in that country, one must look to whether the work is eligible for protection under bilateral treaties, regional treaties or multinational treaties or conventions.[30] Most countries are members of the Berne Convention for the Protection of Literary and Artistic Works,[31] which not only establishes the rules for eligibility for protection in other countries, but binds countries to protect another Berne Convention member's protected works at a minimum level.[32]

There are also other agreements, treaties and conventions that establish eligibility rules and minimum levels of protection for works from one member country by another country where protection is sought. The most significant of these are the TRIPS Agreement in the World Trade Organization's group of agreements dealing with international trade rules,[33] the Geneva Phonograms Convention,[34] the Rome

28. *See* Eric J. Schwartz, Jon A. Baumgarten et al, *Copyright and the Internet: A Primer on Domestic and International Issues*, *available at* http://www.commercenet.com/research/reports/white_papers/87621.html#intl_general (last visited Jan. 28, 2001).

29. *See id.* A foreign work is generally eligible for the same amount of protection as a similar local work. As a result the applicable law to determine the scope of protection for a foreign work is the law of the country where protection is sought.

30. *See id.*

31. *See* Berne Convention for the Protection of Literary and Artistic Works, *available at* http://www.wipo.org/treaties/ip/berne/berne01.html (last visited Jan. 28, 2001).

32. This minimum level is known as "convention minima."

33. *See* The Agreement on Trade-Related Aspects of Intellectual Property Rights (1996), *available at* http://www.wto.org/english/tratop_e/trips_e/t_agm0_e.htm (last visited Jan. 28, 2001). The TRIPS agreement provides for minimum levels of enforcement that must be available in WTO countries for them to meet their WTO obligations and avoid possible trade sanctions under the WTO's dispute settlement regime.

34. *See* Convention for the Protection of Producers of Phonograms Against Unauthorized Duplication of their Phonograms, *available at* http://www.wipo.org/treaties/ip/geneva/geneva.html (last visited Jan. 28, 2001). This treaty establishes minimum copyright protection criteria for sound recordings or phonograms.

Convention,[35] and the new "digital" treaties, the World Intellectual Property Organization (WIPO) Copyright Treaty and the WIPO Performances and Phonograms Treaty.[36] Title I of the DMCA implements both treaties, which provide copyright protection for United States works abroad,[37] in addition to giving authors the exclusive right to authorize their works for availability over the Internet. The copyright laws of each country, together with all of these treaties, establish the basis for copyright protection throughout the world.

II B. General Internet Technology Background

Nothing in recent history has forced a reevaluation of copyrights in the technological age like the Internet.[38] The digitization of copyrighted material allows for instant "perfect" copies of original works to be transmitted from one personal computer to another over the Internet. These copies can then be delivered to millions of users at an exponential rate.[39]

35. *See* The Rome Convention for the Protection of Performers, Producers of Phonograms and Broadcasting Organizations, *available at* http://www.wipo.org/treaties/ip/rome/rome.html (last visited Jan. 28, 2001). This treaty establishes rules for performances, sound recordings/phonograms and for broadcasts. The U.S. is not a party to the Rome Convention.

36. *See* WIPO Copyright Treaty (1996), *available at* http://www.wipo.org/treaties/ip/copyright/copyright.html (last visited Jan. 28, 2001), WIPO Performances and Phonograms Treaty (WPPT) (1996), *available at* http://www.wipo.org/treaties/ip/performances/performances.html (last visited Jan. 28, 2001). These treaties clarify and extend protection offered under the Berne and TRIPS treaties but, most significantly, allow copyright owners to use encryption technology to protect their rights and make breaking the encryption by others illegal. Both treaties were ratified by the required thirty countries by early 2002 the WIPO Copyright Treaty goes into effect March 6, 2002 and the WPPT goes into effect on May 20, 2002.

37. The Berne Convention, however, does not cover sound recordings primarily due to the fact that, unlike the United States, many countries do not believe that sound recordings are works of sufficient originality. *See* Copyright: Cases and Materials 851 (5th ed. 1999).

38. The US Department of Defense developed the Internet in the 1960's for experimental use by the military. It is an international network of computer networks that communicate through various protocols. The Internet is not owned by any particular entity. Anyone with a computer, modem, web browser and Internet connection can access the Internet. As of January 2001 there were over 4 million websites and over 80 million unique Internet users in the US alone according to the Internet statistics leader Media Metrix.

39. *See* Matt Richtel, *Survey Shows Overseas Use of Napster Outstrips U.S.*, N.Y. Times, Apr. 5, 2001, at C4. In February 2001, 26 million people downloaded songs through the Napster system with 8.5 million people accessing the service daily.

The Internet allows infringement of nearly all forms of copyrighted materials, but music has been one of the most dramatically affected industries thus far.[40] With the advent of streaming, digital downloads and compression technologies music has become an on demand commodity on the Internet.[41] This creates both an opportunity and a dilemma for music copyright holders. Copyright owners have the opportunity to develop profitable digital distribution systems for music that will allow for inexpensive, efficient transfer of copyrighted musical compositions to consumers.[42] The industry also faces the dilemma, however, of significant potential for rampant copyright infringement with limited technological ability to stop it.

The development of MP3 technology is a major factor in the current legal disputes over file sharing on the Internet. MP3 is a digital compression technology which stands for MPEG-1 Audio Layer 3.[43] Compression technologies such as MP3 allow audio data, which generally requires large files, to be compressed into relatively small files that are easily transferred across the Internet and downloaded onto a personal computer. These files are digital, so they retain near CD-quality sound no matter how many copies are made, and once downloaded can be played through a computer or other MP3 compatible device

40. As one indication of this, in late 2000 the term "MP3" replaced "sex" as the most frequently searched word on the Internet according to Media Metrix.

41. There were an estimated 500 million songs downloaded from mid 1999 through mid 2000 alone according to the Media Metrix Plug In Report: *Fact and Perspectives on the Music Player Market* (July 2000), *available at* http://us.mediametrix.com/data/jupitermediametrix.pdf (last visited Jan. 29, 2000). The important distinction between streaming and downloading music files over the Internet is that streaming music is simply a performance of the music whereby it passes through the users computer and the music is never left on the users hard drive. A copy is never created. When a song is downloaded, a digitally cloned copy of the file is transferred to the users hard drive. Digital compression decreases the size of the file without significantly impacting the quality of the music such that would be large files can be quickly and easily transferred over the internet.

42. In fact, as of November 2000, all of the major music companies had deployed or would soon deploy digital distribution programs. Most of them include the release of a small number of albums and a larger number of "singles" available for commercial download at various retail sites and portals on the Internet. The industry viewed these programs as "tests" and to date the consumer experience has proven to be far more cumbersome and far less popular than Napster. As of Early April 2001, the record labels announced their next steps, which include subscription services, *see* discussion *infra* at p. 237.

43. "MP3" stands for Motion Picture Experts Group or MPEG-1 Audio Layer 3. It is a compression technology. *See* http://www.mpeg.org for additional information.

any time the listener wishes.[44] Free MP3 software applications available on the Internet allow users to encode songs from their own CD collections by "ripping"[45] the files from their CDs into the MP3 format and placing the files on the users hard drive thereby allowing users to trade songs across the Internet. People using this process almost never have permission from copyright owners to make digital copies of their music available on the Internet, and as such they are directly infringing music copyrights.[46]

Although it is fairly easy to encode MP3 files using a CD audio disc and a computer with the proper software,[47] the wide spread acceptance and proliferation of illegal MP3 trading has grown exponentially in the last two years due to a technology called peer to peer (P2P) file sharing.[48] Simply put, the technology allows users to exchange content over the Internet directly from one users' hard drive to another. Prior to the advent of P2P file sharing, pirated content was only available through a direct download of the file to the users' hard drive from a website hosted on a central web computer.[49] In this model, the users' computer is the "client" and central computer is the "server." In the P2P model, the users' computer acts as both client and server.[50] Napster is just one permutation of a P2P file sharing software.[51] It allows end users to post and share music files with other users. Users search for a particular music file and the software tells them on what other users' hard drive the file is available, and at what connection speed. Once the file is downloaded, it becomes another source for other users to download unless dictated otherwise. Napster and other

44. *See id.*

45. Ripping is the process of removing files from one format such as a CD and encoding them in another such as an MP3 file.

46. *See* discussion of direct copyright infringement *infra at p. 213.*

47. Some of the most popular free software applications used for recording and playing MP3's include Nullsoft's WinAmp Player, Microsoft's Windows Media Player, Real Network's Real Audio Jukebox and the MusicMatch player. Essentially these applications act as a desktop digital recorder, player and database where a user can record, catalog and listen to hours of MP3's in their own computer "jukebox."

48. *See* Alan Zeichick, *P2P Networks Explained*, RED HERRING, Dec. 4, 2000.

49. *See id.*

50. *See id.*

51. Currently there are hundreds of peer to peer websites offering peer to peer file sharing of music, books, movies and other multimedia files. Some examples include: Gnutella, I-Mesh, Flycode, Angry Coffee, Onshare.com, LightShare.com and others.

P2P software do let users shut down access to their files so that no one can take a file off their computer against their will.[52]

Strictly speaking, Napster isn't completely P2P. It uses servers to provide directory services for file locations. Pure P2P systems simply use a network of computers as hosts that pass requests and information directly to one another.[53] This simple structural detail of the Napster system is one of its "fatal flaws" in its legal argument against contributory infringement discussed infra. Since Napster servers are a necessary element to indexing and searching for song titles, they cannot rightfully claim that the file exchange occurs solely between two private individual users.[54]

The combination of P2P file sharing software with MP3 compression has created the current legal and technological dilemma. Since MP3 files generally contain no copyright management system they offer no protection against unauthorized copying, use or distribution. Without copyright management information, it is impossible to determine who exactly is infringing or how many copies of copyrighted materials are being made. Recently developed compression technologies have "digital rights management" (DRM) systems built into their audio formats.[55] Digital rights management allows content providers of copyrighted materials to impede unauthorized replication of a digital work by setting certain rules by which the content can be accessed. Rights management technologies are in the early test phase and show promise in protecting digital files.[56] The protection offered by DRM's is limited, however, by the technology of the hardware or software that interacts with the digital files. In other words, a properly protected file may lose all of its DRM protection if played on an MP3 player or porta-

52. *See* Zeichick, *supra* note 48.

53. *See id.*

54. *See* Colin Beavan, *Lock Up Your Content*, INSIDE, Dec. 12, 2000, at 74.

55. There are several digital rights management technologies currently in use, including the Microsoft's popular Windows Media Player DRM, as well as technologies developed by companies such as Reciprocal, Intertrust and many others. Although Digital rights management technology is critical to a solution for secure digital music files, in the wake of the downturn in the "internet economy" of 2001, many of the companies that developed the technology have folded or suffered including both Reciprocal and Intertrust.

56. *See* Media Metrix Plug In Report: *Fact and Perspectives on the Music Player Market* (July 2000), *available at* http://us.mediametrix.com/data/jupitermediametrix.pdf (last visited Jan. 29, 2000).

ble device[57] that does not support the particular DRM used to protect the file.

Another type of rights management technology is called watermarking. The basic purpose of digital watermarking is to encode data within the digital format about the author, the copyright date, and permit uses of the material.[58] When used in conjunction with tracking tools, copyright owners are able to track down and potentially prosecute infringers. Digital watermarking does not prevent copying in the first instance, and therefore does not safeguard against unauthorized copying. Another drawback of watermarking is that digital files that are already in the marketplace[59] without watermarking technology can be digitally copied without being traced or protected.

There are several other types of digital rights technologies available or in development,[60] but given the current state of the hardware[61] and software,[62] none solve the current problem of digital copyright

57. Portable devices are similar to portable cassette or CD players, but instead play MP3 files that can be transferred from a users' computer to the particular device and then enjoyed wherever the user chooses. Some popular brands currently include the Rio Riot, the Nomad, Sony's Memory Stick, and the very popular Apple i-Pod.

58. Companies such as Verance, Liquid Audio and others have developed their own proprietary watermarking technologies and are currently the most widely used by the music industry. Generally, watermarking encodes inaudible audio bits into the music file that identify the file. It is imperceptible to the listener but can be detected by a DRM loaded on a computer.

59. At this point, the phrase "digital files that are already in the marketplace" dauntingly encompasses nearly all audio tracks currently available on CD which is in essence the history of recorded music to date.

60. These include Intertrust's "Digibox" and other "digital wallet" technologies. These type of technologies lock the copyrighted content in a "virtual" box and sets specific rules as to how and by whom the content can be accessed depending on how much the user paid to access the content. The content may be accessible for an hour, a day, a week or indefinitely depending on the business rules set by the copyright holder. The user gets a "digital key" which is tied to their hard drive so that only that individual user may unlock the content on their computer. If the file is transferred to another hard drive via download or other method, the file will be useless without the key.

61. Hardware includes personal computers, portable MP3 players, cell phones and other wireless devices. The music industry created the Secure Digital Music Initiative (SDMI) to develop hardware that has standard copyright protection features. SDMI was a consortium of over 120 organizations of international electronics and music companies with the goal of developing a voluntary, open framework technology for standard copyright protection on all hardware capable of playing digital music. The group ultimately had little impact on the proliferation of unprotected music through the Internet and disbanded in 2001. While many portable devices are now "SDMI compliant" most still allow a user to play non-SDMI protected files.

62. Software includes audio CD's and unsecured MP3 files.

infringement. Even if secure digital rights technologies do succeed in protecting copyrights on-line there still remains the question of whether these technologies will be accepted by consumers. If they are, additional questions about fair use rights arise, which are discussed infra.[63] If consumers reject these protective measures in favor of unsecured digital technologies, copyright owners will have to contend with Internet piracy with limited technological ability to prevent infringement.

II C. Napster's Defense

It is within this background of copyright protection and technology in both the United States and abroad that the Napster suit arose. Napster made several arguments in defense of its file sharing system. Its principal defense argument was that there was no direct copyright infringement by Napster users.[64] Direct copyright infringement occurs when a party violates any of the copyright holder's exclusive rights.[65] Napster claimed that its users were not infringing copyrights, but instead they were making "fair use" of the copyrighted works when they downloaded music files and traded with other users.[66] Fair use is a defense to copyright infringement.[67] It limits the extent of property interest granted to the copyright holder. This right allows a person or organization the ability to use an excerpt or an entire copyrighted work when used for purposes of teaching, research, news reporting, comment, criticism or parody without express permission from the

63. The consumer will often be cut off from copyrighted materials that they previously had access to after their license for use has expired. When a person currently purchases a CD, they may play it as often as they like in whatever CD players they wish. Consumers are used to the idea of doing what the like with music once they have purchased it and "own" it. It will be difficult for consumers to get used to the idea of limiting the uses of music after they have control over the file for a certain amount of time, but they may have to get used to a more limited idea of fair use.

64. *See* John Heilemann, *David Boies: The Wired Interview*, Wired Magazine, Sept. 2000.

65. *See* 17 U.S.C. § 501(a).

66. *See* Heilemann, *supra* note 64.

67. *See* 17 U.S.C. §107. This doctrine was originally developed as a policy consideration in case law. It was specifically codified in the 1976 Act. Fair use is the most significant and most venerable limitation on an author's copyright prerogatives. The traditional concept of fair use excuses reasonable unauthorized appropriations of a copyrighted work, when the use in some way advanced the public benefit, without substantially impairing the present or potential economic value of the copyrighted work. That being said, there is no real definition of fair use. It is an equitable rule of reason and each case raising a fair use defense must be decided on its own facts.

copyright owner.[68] There is no set formula for determining at the outset whether a use will qualify for the fair use defense. Whether the court allows someone other than the copyright holder to reproduce, distribute, adapt, display and/or perform copyrighted works depends upon four factors: (1) the purpose and character of the use (commercial purposes, non-profit, educational); (2) the nature of the copyrighted work; (3) the "amount and substantiality of the portion used" in relation to the work as a whole; and (4) the effect of the use upon the potential market for the work or the value of the work.[69]

In general, commercial "for profit" uses are not considered fair use.[70] A person is not allowed to take the "value" of a work without permission and sometimes that value is found even in a short clip or excerpt.[71] The Court of Appeals did accept a portion of Napster's fair use argument that the service does have substantial non-infringing uses,[72] but this argument was not enough to demonstrate a complete fair use defense. In the end, the court rejected Napster's fair use argument based on all four factors.[73]

Although the Court of Appeals requested that the district court modify the original injunction with relation to Napster's liability for contributory infringement, the court held that Napster would likely be found liable for contributory infringement after a full trial.[74] Contributory copyright infringement occurs when a person or entity,[75] with knowledge of the infringing activity, induces, causes, or materially contributes to the infringing conduct of another.[76] Contributory infringe-

68. *See id.*

69. *See id.* 17 U.S.C. §107 lists the factors to be considered in determining fair use.

70. *See* Sony Corp. of America v. Universal City Studios, Inc., 464 U.S. 417 (1984). Justice Stevens noted that if Sony's copying was "for a commercial or profit-making purpose, such use would presumptively be unfair."

71. Even a 3-second song clip may not be considered fair use under certain contexts. Thus, the context is critical to a fair use analysis.

72. The major "non-infringing" uses that Napster argued included the authorized use of copyrighted works by new artists who benefited from the exposure, as well as "sampling" and "time shifting," the principle "fair use" defense upheld in the infamous *Sony Corp. of America v. Universal City Studios, Inc.* case.

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

74. *See id.*

75. For copyright infringement on the Internet, the usual "entity" is an ISP.

76. The classic explanation of the contributory infringement doctrine is explained by Judge Anderson in Gershwin Publishing Corp. v. Columbia Artists Management, Inc., 443 F.2d 1159 (2d Cir. 1971), where he stated "one who, with knowledge of the infringing activity, induces, causes or materially contributes to the infringing conduct of another, may be held liable as a "contributory" infringer."

ment extends liability beyond the direct infringer and imposes liability equally on other parties who contributed to the infringement.[77] The court determined that Napster had actual and constructive knowledge of its users infringing activity and was thus liable for the actions of its users.[78] The court requested a modification of Napster's liability for contributory infringement based on the fact that just because a technology has significant infringing capabilities does not make its operator liable for contributory infringement unless the system operator is aware of the specific infringement.[79] Hence, the district court had to modify the order to include notification by the RIAA to Napster of the specific copyrighted works that its users infringed.

In accordance with Napster's general denial of any direct infringement by its users, Napster also argued that it therefore could not be liable for vicarious copyright infringement.[80] Vicarious infringement expands the scope of liability to third parties not directly infringing. Vicarious infringement occurs when an entity or person has the ability to control the activities of a direct copyright infringer and also receives a financial benefit from the infringing activities, but does not prevent the infringement.[81] Liability may be imposed in this situation, even if the entity is unaware of the infringing activities. Unlike contributory liability, where the behavior and intent of the defendant determines liability, under a vicarious liability theory, the relationship between the defendant and the direct infringer determines the defendant's liability.[82] The court determined that Napster does have the ability to supervise and control its users and that Napster derived a direct financial benefit through the infringing activity, which attracted its large user

77. The Copyright Act itself does not specifically mention "contributory infringement," but as Justice Steven's explains in *Sony* at 435, "the absence of such express language in the copyright statute does not preclude the imposition of liability for copyright infringements on certain parties who have not themselves engaged in the infringing activity. For vicarious liability is imposed in virtually all areas of the law, and the concept of contributory infringement is merely a species of the broader problem of identifying the circumstances in which it is just to hold one individual accountable for the actions of another."

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

79. *See id.*

80. *See id.*

81. See David N. Weiskopf, *The Risks of Copyright Infringement on the Internet: A Practitioner's Guide*, 33 U.S.F. L. REV. 1, at 8 (1998).

82. *See id.*

base.[83] Thus Napster was found liable for vicarious copyright infringement.

Napster also asserted a statutory limitation defense against liability based on §512 of the DMCA.[84] They argued that they are covered by the "safe harbor" provision given to ISP's so that they are not responsible for their user's activities.[85] The RIAA argued that the DMCA did not afford Napster this protection because Napster was guilty of contributory and vicarious infringement.[86] The court rejected the RIAA's argument stating, "we need not accept a blanket conclusion that §512 of the Digital Millennium Copyright Act will never protect secondary infringers."[87] The court expressly did not want to create a *per se* rule whereby an entity who may be liable for vicarious or contributory infringement is ineligible for application of §512, but instead they opted for a case by case analysis.[88] Based on the facts of this case, where it is unclear whether Napster fits the definition of an ISP under §512[89] and the balance of equities falls in favor of the RIAA, the court was ultimately unwilling to allow Napster the protection of the DMCA "safe harbor" provision.

Napster's final significant defense argument was copyright misuse.[90] By attempting to prevent Napster's users from downloading and trading music files, Napster claimed that the music industry is using their copyrights for anti-competitive purposes.[91] In essence, Napster argued that the music industry was trying to gain control over Napster through their copyrights and that this is copyright misuse.[92] As with the rest of Napster's affirmative defenses, however, the court rejected

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

84. *See id.*

85. *See* 17 U.S.C. §512 (1998).

86. *See A & M Records,* 239 F.3d at 1025.

87. *See id.*

88. *See id.*

89. *See id.* The court stated: "Plaintiffs have raised and continue to raise significant questions under this statute, including: (1) whether Napster is an Internet service provider as defined by 17 U.S.C. § 512(d); (2) whether copyright owners must give a service provider "official" notice of infringing activity in order for it to have knowledge or awareness of infringing activity on its system; and (3) whether Napster complies with § 512(i), which requires a service provider to timely establish a detailed copyright compliance policy."

90. *See A & M Records,* 239 F.3d at 1026.

91. *See* John Heilemann, *David Boies: The Wired Interview*, WIRED MAGAZINE, Sept. 2000.

92. *See id.*

this argument as well stating, "there is no evidence here that plaintiffs seek to control areas outside of their grant of monopoly. Rather, plaintiffs seek to control reproduction and distribution of their copyrighted works, exclusive rights of copyright holders."[93] With this final argument cast aside, the court affirmed the injunction to prevent what it perceived to be the continued harm caused by the Napster system and also remanded to the district court to narrow the injunction as discussed *supra* in Part I.

III A. The Napster Case in the International Context

Based on the foregoing discussion, the Court of Appeals applied relatively straightforward U.S. copyright law principles in a very systematic, reasoned fashion. While there are arguments on both sides of the question, there were no issues of first impression and the court's legal reasoning was not particularly controversial. Could the same be said if a copyright infringement suit arose in which Napster were to take its service abroad and run it from a foreign country, yet still allow access to U.S. based users? How would the RIAA enforce its judgement or legally prevent a similar service not currently enjoined that is operating overseas? Some of the World Intellectual Property Organization's and World Trade Organization's treaties discussed *supra* in Part IIA would likely play a role in a foreign copyright infringement action of this nature. Since these treaties have not been ratified in all foreign countries, however, they may be of little help.[94] The copyright law of the individ-

93. *See A & M Records,* 239 F.3d at 1027. In February 2002, the district court denied the RIAA's motion for summary judgement and granted Napster more time for discovery on two issues seemingly disposed of by the Court of Appeals ruling. Napster claims that many of the titles that the music companies assert copyrights in are not owned by them and that the music industry's conduct since the Court of Appeals ruling lends credibility to their copyright misuse argument. The district court agreed based on antitrust concerns raised by the industry's own on-line music ventures MusicNet and Pressplay. The district court stated, "these ventures look bad, smell bad and sound bad. If Napster is correct these plaintiff's are attempting near monopolization of the digital distribution market." If Napster is successful in showing illegal collusion, they could invalidate the music industry's lawsuit. *See* Matt Richtel, *Napster Wins One Round in Music Case: Judge Questions Tactics of Major Record Labels*, N. Y. Times, Feb. 23, 2002, at C1.

94. The international community adopted two new treaties in 1996 to bring copyright protection into the digital age, the WIPO Copyright Treaty (WCT) and the Performers and Phonograms Treaty (WPPT). The WPPT provides protection against unauthorized reproduction, distribution, and rental of recorded music. It requires the copyright holder's consent to make sound recordings available over the Internet. In addition, copying or hacking of technical measures to prevent unauthorized copying is prohibited. Thirty countries must ratify the treaties for them to enter into force. Both

ual country where the infringing service is based would apply. How would this potential choice of law conflict play out in the United States? Four significant legal doctrines are the primary concerns to answer these questions in a case of international copyright infringement. These include (1) the presumption against extraterritoriality,[95] (2) personal jurisdiction,[96] (3) forum non-conveniens[97] and (4) choice of law.[98]

The presumption against extraterritoriality deals with the hesitancy of U.S. courts to apply U.S. law in cases involving foreign or American actors on foreign soil. It is a principle of international law that national laws cannot extend beyond its own territories.[99] The main policy behind the presumption is that by keeping the impact of U.S. law within the United States, the courts not only avoid potential conflict between the U.S. and foreign nations, but also avoid difficult choice of law issues that would otherwise arise.[100] The various international copyright treaties discussed *supra* are additional reasons why U.S. courts are reluctant to apply U.S. law to foreign infringement cases. Since the various WIPO treaties and the TRIPs agreement are based on minimum rights and since each nation's intellectual property laws are assumed not to apply extraterritorially, a non-extraterritorial approach makes sense.[101] If U.S. courts applied U.S. law to international copyright infringement cases, it would effectively render the various treaties meaningless.[102]

---

treaties were ratified in early 2002 and will go into effect in signatory countries by mid-2002.

95. *See* Curtis A. Bradley, *Extraterritorial Application of U.S. Intellectual Property Law: Territorial Intellectual Property Rights in an Age of Globalism*, 37 VA. J. INT'L L. 505, 583 (1997).

96. *See* Stephan Wilske and Teresa Schiller, *International Jurisdiction in Cyberspace: Which States May Regulate the Internet?*, 50 FED. COMM. L. J. 117, 139 (1997).

97. *See* Brenda Tiffany Dieck, *Reevaluating the Forum Non-Conveniens Doctrine in Multi-territorial Copyright Infringement Cases*, 74 WASH. L. REV. 127 (1999).

98. *See* Andreas Reindl, *Choosing Law in Cyberspace: Conflicts on Global Networks*, 19 MICH. J. INT'L L. 799 (1998).

99. *See* William S. Dodge, *Understanding the Presumption Against Extraterritoriality*, 16 BERKELEY J. INT'L L.85 (1998).

100. *See* Bradley, *supra* note 95.

101. *See id*; *see also* MARSHALL A. LEAFFER, INTERNATIONAL TREATIES ON INTELLECTUAL PROPERTY (2d ed. 1997).

102. *See* Bradley, *supra* note 95.

Courts have consistently held that U.S. copyright law does not apply beyond U.S. territorial boundaries.[103] This principle was recently applied in *Subafilms, Ltd. V. MGM-Pathe Communications* Co.[104] In that case, the court held that the mere authorization within the United States of acts of infringement occurring outside of the United States does not violate U.S. copyright law.[105] Overruling an earlier decision,[106] the court held that an "authorization" only violates the Copyright Act if the authorized conduct itself takes place within the boundaries of the United States.[107]

Under this doctrine, a non-U.S. based Napster may not be able to be reached by a U.S. court where the system is not within U.S. boundaries and the infringement (copying and trading of music files by its users) takes place outside of the United States. If U.S. based users downloaded files from a foreign Napster system, they would be liable for direct infringement.[108] It would be impracticable to sue Napster's users individually, however, so another theory of infringement would have to be employed. An exception to the presumption against extraterritoriality in the application of copyright law is extraterritorial conduct that actively induces or contributes to infringement occurring within the United States.[109] Since Napster was found liable of contributory infringement and it is likely that even a non-U.S. based Napster would also be similarly liable, a plaintiff would be able to overcome the presumption.[110] It would be very difficult, however, to fall within this

103. *See* Bradley, *supra* note 95. *See, e.g.*, Subafilms, Ltd. v. MGM-Pathe Communications Co., 24 F.3d 1088, 1093 (9th Cir. 1994) (referring to the "undisputed axiom that United States copyright law has no extraterritorial application").

104. 24 F.3d 1088 (9th Cir. 1994).

105. *See Subafilms, Ltd.*, 24 F.3d 1088. The court noted that "there is no clear expression of congressional intent in either the 1976 Act or other relevant enactments to alter the preexisting extraterritoriality doctrine." The court also warned that extraterritorial application of U.S. law could also send a signal to other countries that the U.S. does not trust their enforcement mechanisms.

106. *See* Peter Starr Prod. Co. v. Twin Continental Films, Inc., 783 F.2d 1440 (9th Cir. 1986).

107. *See Subafilms, Ltd.*, 24 F.3d 1088.

108. *See* 17 U.S.C. § 501(a).

109. *See, e.g.*, Cable/Home Communication Corp. v. Network Prods., Inc., 902 F.2d 829, 845-46 (11th Cir. 1990); Metzke v. May Dept. Stores Co., 878 F. Supp. 756, 760-61 (W.D. Pa. 1995).

110. Outside of this specific exception, courts consider 3 factors to determine if the presumption should not be applied: (1) whether there will be adverse effects in the United States if the statute is applied extraterritorially, (2) whether extraterritorial ap-

exception if the majority of the infringement took place in other territories outside of the United States.[111]

Assuming the RIAA were to get over the hurdle of the presumption against extraterritoriality, the next issue to address would be personal jurisdiction. Personal jurisdiction is always an issue in any online copyright infringement lawsuit. In the international context, it is definitely more complicated to determine.[112] Generally, U.S. courts apply the "minimum contacts test" to determine whether exercising jurisdiction over a particular defendant is appropriate.[113] While there are various factors considered under the test, the two key elements in the international context are whether the defendant "purposefully availed themselves of the benefits and protections of the forum state"[114] and ultimately whether exercise of jurisdiction is reasonable.[115]

The problem with personal jurisdiction, in the on-line context, is that it is often difficult to determine whether infringers in Europe, who have established a website targeted to Europeans, but that is also accessible to citizens of other nations including the United States, actually "purposefully availed" themselves of the laws of the United States. This

plication of the law will result in international discord and (3) whether the conduct sought to be regulated occurs largely within the United States.

111. Granted, the United States is the largest music market in the world so Napster without the U.S. is certainly less attractive economically to its developers, but the music market outside the U.S. is still quite significant and would potentially present a similar negative impact on sales that the RIAA alleged in their *A & M Records, Inc. v. Napster, Inc*. suit.

112. *See* Wilske & Schiller, *supra* note 96.

113. *See, e.g.,*Pennoyer v. Neff, 95 U.S. 714, 722 (1878); International Shoe Co. v. State of Washington, 326 U.S. 310, 316 (1945); World-Wide Volkswagen Corp. v. Woodson, 444 U.S. 286, 297 (1980); Burger King Corp. v. Rudzewicz, 471 U.S. 462, 476-77 (1985); Asahi Metal Industry Co. v. Superior Court, 480 U.S. 102 (1987). These are the cornerstones of a line of U.S. Supreme Court cases that established the "minimum contacts test." The basic policy behind the test is that due process requires a defendant to be subject to a distant court's judgment only if he or she has minimum contacts with the jurisdiction such that exercising jurisdiction does not offend "traditional notions of fair play and substantial justice." The contacts must be "continuous and systematic" whereby the defendant "purposefully availed themselves of the benefits and protections of the laws of the forum state." In addition, the defendant must "know or reasonably anticipate" that their activities could give rise to litigation and the contacts must actually give rise to the litigation. Finally, it is not enough for the minimum contacts to exist, jurisdiction must ultimately be "reasonable" under the circumstances balancing the litigant's interests against the forum's interests.

114. *See* Hanson v. Denckla, 357 U.S. 235 (1958).

115. *See* Asahi Metal Industry Co. v. Superior Court, 480 U.S. 102 (1987).

scenario was recently analyzed in *Playboy Enterprises, Inc. v. Chuckleberry Publishing, Inc.*[116] In that case, an Italian website that had U.S. based subscribers was sued for trademark infringement. The court concluded that even though it could not prescribe conduct on the Internet,[117] since Playboy knew that U.S. citizens used its service, the court was entitled to prohibit access to the site in the United States. Therefore, the defendant was enjoined from offering its magazine to customers residing in the United States.[118] Under this precedent, there is still a case by case analysis necessary, so it is difficult to predict with certainty if a non-U.S. based Napster would be subject to jurisdiction in the United States.

Additionally, under most circumstances there will be an "objective reasonableness" argument to be made where defendants will have to travel thousands of miles to a foreign courtroom to defend themselves against a law suit that they did not reasonably anticipate.[119] Courts are split over Internet conduct that is sufficient to justify jurisdiction, and case law to date has been inconsistent even within the domestic context.[120] Most courts apply the traditional personal jurisdiction principles to the on-line context[121] and this may be problematic for U.S. based plaintiffs looking to enjoin foreign Internet entities. Future case law may have to add more elements to the "minimum contacts test" to account for "cyber-contacts" and establish more clear rules and expectations in this area. In the mean time, it remains to be seen whether a foreign run Napster could be reached by a U.S. court.[122]

---

116. 939 F. Supp. 1032 (S.D.N.Y. 1996).

117. The court stated: "The Internet is a world-wide phenomenon, accessible from every corner of the globe. [Defendant] cannot be prohibited from operating its Internet site merely because the site is accessible from within one country in which its product is banned. To hold otherwise "would be tantamount to a declaration that this Court, and every other court throughout the world, may assert jurisdiction over all information providers on the global World Wide Web."

118. *See Playboy Enterprises*, 939 F. Supp. 1032.

119. *See supra* note 115.

120. *See* Wilske & Schiller, *supra* note 96; s*ee also* Andrew E. Costa, Comment, *Minimum Contacts in Cyberspace: A Taxonomy of the Case Law*, 35 HOUS. L. REV. 453, 502 (1988).

121. *See* Zippo Mfg. Co. v. Zippo Dot Com Inc., 952 F. Supp. 1119 (W.D. Pa. 1997).

122. The answer to this question will be answered shortly by the RIAA's latest lawsuit brought in U.S. District Court for the Central District of California against three file sharing services that arose following Napster's shut down. One of the services, known as KaZazA, is a Dutch company based out of Amsterdam and another called Grokster is based out of the West Indies. Subsequent to the October 2001 suit, KaZazA was then sold to an Australian firm in January 2002. As of March 2002, both KaZazA and Grok-

Assuming the difficulties of personal jurisdiction are tackled, however, the question of what is a convenient forum for the litigation becomes the next major issue. U.S. courts must decide this question through the application of the doctrine of forum non-conveniens.[123] The doctrine requires a case by case analysis and therefore there are no consistent results among certain classes of cases.[124] Since the Internet transcends traditional boundaries, it allows for simultaneous copyright infringement by many users in multiple countries. In this scenario, choosing the most convenient forum to litigate the case is difficult. If a choice can be made and the most convenient forum is in a foreign nation, the U.S. court may dismiss the case in favor of the foreign jurisdiction under the forum non-conveniens doctrine.[125] The problem that arises under the non-U.S. based Napster hypothetical, however, is that since the direct infringement by users and Napster's servers are located in various countries, there may be multiple convenient foreign courts that satisfy the alternative forum element of the doctrine.[126] Unless the plaintiff has significant financial resources, it would be very difficult to litigate in multiple foreign courts. This difficulty creates an atmosphere where in some cases, the costs of infringement may be less than litigating the claim. In this hypothetical, however, the recording industry does have the resources to litigate in foreign territories and the interests at stake are so critical that they would surely make the investment in resolving the suit outside the United States. While it seems likely that this element of the RIAA's difficulties in reaching a foreign Napster would be surmountable, since this factor is also a case by case analysis, the forum non-conveniens issue could prove to be problematic.

---

ster are still defendants in the suit and no motion to dismiss due to lack of jurisdiction by the U.S. court has been filed. For more *see infra* note 167.

123. *See* Brenda Tiffany Dieck, *Reevaluating the Forum Non-Conveniens Doctrine in Multi-territorial Copyright Infringement Cases*, 74 WASH. L. REV. 127at 127 (1999). Dieck describes the doctrine as "a judicially created doctrine that allows the judge, at her discretion, to dismiss a case on grounds of convenience to the parties and the court . . . when the more convenient forum is outside the federal system."

124. *See id*.

125. The leading case on the doctrine is Piper Aircraft Co. v. Reyno, 454 U.S. 235 (1981). The U.S. Supreme Court created the forum non-conveniens test that must be applied in international cases in the *Piper* decision. The Court used a two step analysis, first determining whether an adequate alternative forum exists and if one does exist, then balancing a series of interests.

126. *See* Dieck, *supra* note 123.

If the convenient forum hurdle is successfully passed, the final issue to be determined is what law will be applied to the case, United States law or the foreign country's law? International copyright law and the treaties that make up its core are based on the principle of territoriality.[127] This means that courts must focus on the location where the acts occurred to decide which law to apply.[128] Once again, the Internet context makes the choice of law determination more difficult given that there could be multiple locations where the infringement occurs particularly in a P2P network. The WIPO treaties help with the choice of law quagmire through their requirement of uniform application of copyright laws, but they do not solve the issue especially where either the service, and/or the infringement is based in a country that is not a signatory to the treaty.[129] Here again, there is a case by case analysis, which presents significant potential problems for a U.S. based plaintiff. For example, if a U.S. court determined on the facts of a case that an exception to the presumption against extraterritoriality was justified, those same facts may also militate against a choice of U.S. copyright law.

Based on the foregoing discussion it is uncertain whether an international version of Napster could be enjoined in the United States. After a great deal of complex legal determinations are made, however, it is certainly possible. Even so, legal representatives for the RIAA are likely concerned about this scenario. The more daunting next question is whether after all the international legal issues are resolved, and the RIAA gets a similar judgement enjoining Napster in a foreign court or a U.S. court applying foreign law, is it technologically possible to enforce the judgment?

III B. Real World Examples of Technologies and their Developers that Defy Copyright Enforcement

New technologies have developed to a point whereby copyright infringement is taking place on a massive scale, in multiple countries, simultaneously by anonymous users. Given the pace of technological advances, a world where certain technologies are essentially ungovern-

127. *See* Andreas Reindl, *Choosing Law in Cyberspace: Conflicts on Global Networks*, 19 Mich. J. Int'l L. 799 (1998).

128. *See id.*

129. *See id.*

able by the law is the dawning reality.[130] This scenario is the real challenge to current copyright law and its enforcement.

The challenge is here today in several forms including the Freenet Project.[131] Freenet is the brainchild of Scotland's Ian Clarke. As stated on Freenet's website, "The 'Freenet' project aims to create an information publication system similar to the World Wide Web, but with several major advantages over it based on the [P2P] protocol" developed by Clarke.[132] Freenet is a single worldwide information database that stores, caches, and distributes information based on demand.[133] To participate in the system, users simply need to run a piece of server software on their computer and optionally use a client program to insert and remove information from the system. Anyone can write a client or a server program for Freenet, which is based on an open protocol.[134] The site describes the system's main features as the following:

- "Freenet does not have any form of centralized control or administration.
- It will be virtually impossible to forcibly remove a piece of information from Freenet.
- Both authors and readers of information stored on this system may remain anonymous if they wish.
- Information will be distributed throughout the Freenet network in such a way that it is difficult to determine where information is being stored.
- Anyone can publish information. They don't need to buy a domain name or even a permanent Internet connection.
- Availability of information will increase in proportion to the demand for that information.

130. *See* John Heilemann, *David Boies: The Wired Interview*, WIRED MAGAZINE, Sept. 2000. In response to the idea that new file sharing technologies may be ungovernable, David Boies Napster's lead attorney stated, "I think that's very possible and if it happens, it will have a lot to do with the fact that we live in a world where laws are made by nation-states, but the internet is worldwide."

131. *See* http://freenet.sourceforge.net/.

132. *See The Freenet FAQ: What is Freenet?*, *available at* http://freenet.sourceforge.net/index.php?page=faq (last visited Jan. 29, 2001).

133. *See id.*

134. *See id.* Open Protocol or open source is an internet technology that developers intentionally make freely available for public use without the requirement of licensing fees. This allows other developers to manipulate another's code and transform it for other uses or functionality.

- Information will move from parts of the Internet where it is in low demand to areas where demand is greater."[135]

These features have a direct impact on copyright infringement theories, detection and enforcement. Freenet operates in a decentralized manner and provides users with anonymity. There are no servers to be shut down and it is nearly impossible to identify who is posting copyrighted material. This makes direct, contributory or vicarious copyright infringement claims practically impossible. There is no central index residing on servers as there is with Napster, which give potential litigants a legal foundation for contributory infringement. Unlike the Napster system which is set up in such a way that users can be monitored,[136] Freenet has no way of monitoring the systems users, so liability for vicarious infringement is also very difficult to prove.[137]

In addition, Freenet uses intelligent routing and caching which makes it efficient and scalable. The most popular content is mirrored automatically, so the more requests for a particular file, the more likely it will be accessible to the user.[138] Flooding the network to disrupt information flow will be nearly impossible as well.

When it is impossible to identify the copyright infringer, impossible to shut down a central system and there is no single corporate entity to sue, none of the traditional theories of copyright infringement apply. Even if the specific infringer is identified and successfully prose-

---

135. *See The Freenet FAQ: Why is Freenet Interesting? available at* http://freenet.sourceforge.net/index.php?page=faq (last visited Jan. 29, 2001).

136. *See A & M Records*, 239 F.3d at 1027."Napster may be vicariously liable when it fails to affirmatively use its ability to patrol its system and preclude access to potentially infringing files listed in its search index. Napster has both the ability to use its search function to identify infringing musical recordings and the right to bar participation of users."

137. *See* Declan McCullagh, *Good Gnus in Napster Ruling* (Feb. 14, 2001), *available at* http://www.wired.com/news/print/0,1294,41784,00.html (last visited Apr. 14, 2001). Lack of the ability to monitor may be "a legal opening for file-swapping services such as Gnutella and Freenet, which are set up in a way that prevents their creators from easily patrolling the network and deleting MP3 files at the behest of the Recording Industry Association of America's member firms."

138. Richard Koman, *Free Radical: Ian Clarke Has Big Plans For The Internet* (Nov. 14, 2000), *available at* http://www.oreillynet.com/pub/a/p2p/2000/11/14/ian.html (last visited Jan. 29, 2001). According to Clarke, "one of the things that Freenet does is it actually moves information around and dynamically replicates information to reduce the load on the network bandwidth. So, if 1,000 people in the U.K. request the same document from the U.S. and they were using Freenet, it would only need to travel over the Atlantic once, and thereafter it would be stored locally and distributed within the U.K. - or within Europe, depending on where the demand was."

cuted, once the content is on other anonymous users' systems, how do courts enforce the judgements when the content is impossible to remove? Napster argues that by shutting them down, U.S. courts will actually hasten the proliferation of entities such as Freenet.[139] This has indeed proven to be true,[140] but Freenet's own attitude toward copyright indicates that they will present a problem to copyright owners with or without Napster or other file sharing services. With regards to copyright infringement Freenet's initial website stated:

> While Freenet has the potential to assist copyright infringement, this battle has already been lost. Millions of copyrighted audio and video files are already being traded on the web each day — the absence of Freenet will not change that. Besides, by far the vast majority of copying activity does not take place online, but via old-fashioned, industrial-scale physical CD pressing.[141]

Whether self serving or not, Freenet and its followers do not subscribe to the traditional notions of copyright law, but instead stretch the fair use doctrine beyond its limits.[142] In response to increased publicity of

139. *See* John Heilemann, *David Boies: The Wired Interview*, Wired Magazine, Sept. 2000. According to Boies shutting down Napster will likely, "drive the peer-to-peer central index technology offshore, or to Canada. And because it is noncommercial, once they set up in Canada, there isn't anything you can do in the United States. If they were selling subscriptions in the United States, you could stop it. If they were charging people, you could stop it. If they were soliciting people, you could stop it. But the thing about this is, you don't need to solicit people. They'll just dial up that Canadian address all by themselves. There really is nothing you can do to stop it."

140. As of late 2001, several file sharing services began to fill the gap left by the Napster's closure. The most significant include: Morpheus (2.5 million users), KaZazA (1.5 million users), Audio Galaxy (1.5 million users), Aimster (1 million users), iMesh (1 million users) and Gnutella based systems Limewire/Bearshare (1 million users). Clearly, shutting down Napster or one file sharing network is not the solution to end mass copyright infringement on the internet.

141. *See The Freenet FAQ: But I'm still worried about terrorism / child pornography / libel / copyright infringement* formerly, *available at* http://freenet.sourceforge.net/index.php?page=faq (last visited Jan. 29, 2001).

142. *See The Freenet FAQ: Won't Freenet be a Haven for Pirates and Criminals? formerly available at* http://freenet.sourceforge.net/index.php?page=faq (last visited Jan. 29, 2001). According to the former site: "the network doesn't know the difference between public domain documents like a Shakespeare sonnet or Bach fugue, and copyrighted works like a Stephen King novel or Carlos Santana song. Because it makes sharing the former easier, it also makes sharing latter easier. This is perceived as a threat to traditional publishing and recording industries just as radio was, and the mimeograph, and television, and the photocopier, and magnetic tape, and the compact disc, and the videocassette recorder, and many other technologies that made sharing information

services like Freenet, however, Ian Clarke has redirected his rhetoric with an anti-censorship argument similar to the failed first amendment claim made by Napster.[143] The latest version of the Freenet FAQ states:

> Of course much of Freenet's publicity has centered around the issue of copyright, and thus I will speak to it briefly. The core problem with copyright is that enforcement of it requires monitoring of communications, and you cannot be guaranteed free speech if someone is monitoring everything you say. This is important, most people fail to see or address this point when debating the issue of copyright, so let me make it clear:
>
> **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.[144]

With statements like this, it is clear to see the difficult challenge facing current copyright laws and enforcement.

A significant drawback to Freenet's technology, which makes it somewhat less of a threat in the short term, is that it is not simple to use.[145] Would-be copyright infringers without a computer science degree have choices; the new rising technology called Aimster[146] is one of them.[147] The software was developed in America, but like all Internet applications it has worldwide implications. Aimster is a cross be-

---

easier. Freenet doesn't do anything different from what can already be done with those technologies, it just does it more efficiently. 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."

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

144. *See The Philosophy Behind Freenet*, *available at* http://freenetproject.org/cgi-bin/twiki/view/Main/Philosophy#CopyWrong (last visited Apr. 14, 2001).

145. *See* Colin Beavan, *Lock Up Your Content*, INSIDE, Dec. 12, 2000, at 73. "Freenet would scare the bejesus out of the music industry — except you need to be a virtual MIT egghead to work [it]."

146. Aimster is now known as Madster. AOL brought a complaint against Aimster claiming that they infringed the trademark for AOL's instant messaging system AIM. A National Arbitration Forum panel ruled in May 2001 that Aimster must relinquish its domain name to America Online (AOL). Aimster appealed the ruling in court, but ultimately gave up the name under a settlement with AOL and changed their name to Madster.

147. *See* Beavan, *supra* note 145, at 73.

tween AOL's Instant Message Service[148] and Napster. The danger in this new technology, both legally and practically, is that it lacks the central index server of the Napster system, but unlike Freenet it is very easy to use.[149] The system operates like a rudimentary search engine that searches a "buddy's"[150] hard drive for a matching list of files that may include audio, video, graphics, text or nearly anything else.[151] When the user finds something they are interested in, they double click on the file name; this establishes a P2P connection that begins the file transfer.[152] A significant difference between this technology and Napster is that the search function is limited to only a relatively small group of users' hard drives at a time, which is closer to falling within the traditional idea of the fair use defense because users are not exposing music files to millions of users at a time.[153] Essentially, the universe of possible infringement is limited to small "cells" of buddies. There are public-domain programmers, however, that are developing plug-ins[154] that will enable file sharing beyond a restricted instant message group, using a distributed index similar to Freenet.[155] In other words, Aimster will allow the same widespread file sharing as Napster, but without its legally vulnerable central index. In addition, Aimster's developers are making future versions compatible with the many com-

148. Instant Messaging (IM) allows one user to communicate directly with another in real time using text messages over the Internet.

149. *See* Beavan, *supra* note 145, at 72.

150. A "buddy" is an IM user selected by another IM user to have access to their instant message system. Buddies are identified by a unique screen name and the screen name is placed in an IM users' "buddy list." The IM application will detect whenever a users' buddies are on-line using the IM system and automatically notify any other users who have that buddy on their list.

151. *See id.*

152. *See id.*

153. *See id.* "Frank Creighton, the RIAA's senior vice president and director of anti-piracy, says that while Aimster 'isn't less harmful or wrong' than using Napster, he allows that 'it is more akin to the days when kids would make compilation tapes and trade them with dorm buddies. It's more like a Phish fan saying, 'I made you this tape. Now I want you to go out and buy the album.'"

154. A plug-in is usually a small piece of software that adds features to a larger piece of software. Common examples are plug-ins for web browsers. The idea behind plug-in's is that a small piece of software is loaded into memory by the larger program, adding a new feature to the larger application. The user need only install the few plug-ins that they need, out of a much larger pool of possibilities, to get custom functionality. Plug-ins are usually created by people other than the publishers of the software the plug-in works with.

155. *See* Beavan, *supra* note 145, at 72. According to Johnny Deep, "Aimster clearly has non-copyright-infringing uses, and he can't help it if public-domain programmers release plug-ins that allow the promiscuous swapping of copyrighted files."

peting instant message technologies.[156] This will allow users to message each other and transfer files across multiple, disparate messaging platforms.[157] A multi-platform Aimster creates the ability to share files among 140 million current instant message users, a user base which is twice the size of Napster's peak membership.[158]

Further exacerbating the legal arguments against Aimster is the fact that the application has various non-copyright infringing uses; the most obvious among them is the instant message function.[159] Other examples that may well fall under fair use include, people who want to share files among multiple computers and store them on Aimster, or co-workers who collaborate on documents together. If Aimster is confronted with a suit seeking an injunction,[160] this fact will allow them to raise the argument that Aimster is similar to the VCR in the infamous *Sony Corp. of America v. Universal City Studios, Inc.,* even more credibly than Napster has argued.[161]

After analyzing some of the decisions in the Napster suit, Napster attorney David Boies[162] advised Aimster to start encrypting all of the information that is exchanged between users on its network.[163] Ironically, this makes monitoring impossible without circumventing the en-

156. *See id.*

157. *See id.*

158. *See id.*

159. *See id.* Legal experts cautiously concur with this idea. "I think the Aimster technology has substantial non-infringing uses," says Julie Cohen, an associate professor of Internet copyright law at the Georgetown University Law Center. Mark Radcliffe, a Palo Alto-based copyright attorney, views Aimster's chances in a post-Napster universe as positive too. "I could foresee a situation where the court rules against Napster, but the judgment is written in such a way that it doesn't affect technologies such as Aimster."

160. In response to a suit brought by Aimster for a declaratory judgement that their service is legal, the RIAA filed a lawsuit against Aimster in the U.S. District Court for the Southern District of New York in May 2001. The RIAA claims that "Aimster provides the same functions as Napster" and "the experience is virtually identical in terms of being able to search the [Aimster] network for other peoples' music." In addition, the RIAA asserts that "the evidence will show that Aimster was as aware as Napster that it was facilitating widespread infringement." *See* Matt Richtel, *Aimster Heads Down a Path Already Taken by Napster: But Music Industry Victory is Not So Certain*, N. Y. TIMES, June 1, 2001, at C1.

161. A technology may be exempt from contributory copyright infringement liability if it has "substantial non-infringing uses." *See* Sony Corp. of America v. Universal City Studios, Inc., 464 U.S. 417 (1984).

162. David Boise represents both Napster and Aimster in their suits against the RIAA.

163. *See* Brad King, *Napster Clone's Curious Terms* (Mar. 2, 2001), *available at* http://www.wired.com/news/print/0,1294,42105,00.html (last visited Apr. 14, 2001).

cryption technology, which violates the DMCA.[164] Thus copyright owners cannot monitor Aimster to see if their rights are being infringed without violating the very law that was passed to protect them.[165] Aimster has learned from watching Napster's legal troubles and is developing a system that falls between the cracks of current copyright law. A statement by Aimster's developer, Johnny Deep, makes a compelling case.

> "They would have to change the law to shut us down, because we comply with the law right now. The copyright owners can go to Congress and ask them to change the law, but right now, they can't shut us down. And I doubt that Congress is going to roll back the safe harbor provisions in the DMCA to shut this down. The product we are offering is the encrypted virtual private network that has incredible non-infringing uses."[166]

All of this leads to a very uncertain picture for music copyrights in the Internet context.

IV. The Legal, Technological and Creative Solutions to On-Line Copyright Infringement

Technology has always forced copyright laws to evolve in reaction to new ways of duplicating and sharing information, but the Internet has upped the ante. Freenet, Aimster and more recent file sharing technologies such as Gnutella and FastTrack,[167] which filled the void

164. *See id.* "Breaking the encryption is illegal under the DMCA because the network and its programming code are copyrighted." *See supra* notes 22, 23.

165. *See id.*

166. *See id.*

167. Both Gnutella and FastTrack are two file sharing technologies that rose to prominence after Napster voluntarily shut down in July 2001. Unlike Napster, Gnutella does not use a central server to keep track of user files. It is a completely decentralized peer-to-peer file transfer network with a shared file directory. As such, it is generally disorganized and inefficient. Gnutella is based on an open source code and is developed by independent volunteer programmers throughout the world. These programmers have started GPulp, which stands for General Purpose Location Protocol, a program that would standardize the music-swapping program and make it much easier to use. Developers are constantly working to improve Gnutella's basic code and the technology is getting better. Since no central entity or computers are involved, a Gnutella based network is essentially impossible to shut down without removing the individual computers from the network. Various file sharing communities including Limewire, Bearshare and Morpheus now use the Gnutella technology. For more on Gnutella, *see Understanding Peer-to-Peer Networking and Modern Peer-to-Peer File Sharing over*

left after Napster shut down, create scenarios whereby the traditional American ideas of copyright infringement are difficult to apply. Those who claim that "copyright is dead," and cannot stop file sharing[168] however, need only read the 9th Circuit decision upholding the Napster injunction and analyze the subsequent repercussions upon Napster to see that American copyright law is alive and well and works as it always has. When the infringing technology is based in a foreign country, this presents an additional challenge because American copyright law may not apply. Thus, U.S. courts must more readily presume extraterritoriality of laws and jurisdiction in order to compensate when an international treaty is not enough to prevent infringement. This alone does not resolve the situation, however, because new technologies are being created to fall outside of American copyright protection. Therefore, current U.S. copyright law, even when applied extraterritorially, does not solve the infringement problem. Even if a court determines

the Internet, available at http://www.limewire.com/index.jsp/p2p (last visited Mar. 14, 2002).

FastTrack was developed in Holland. It differs from Gnutella in that it uses a new peer-to-peer structure that includes "supernodes." A supernode is essentially a powerful peer computer within the network that is used as a centralized index of files for a specific branch of the network. The supernodes can communicate among themselves as well and pass search requests between different branches of the network. FastTrack chooses which computers are supernodes and can do so without the knowledge of the user. Generally, the more bandwidth available to a peer the more likely it will be chosen as a supernode. The supernodes are not centralized and therefore are not under the control of FastTrack. Once a supernode helps the user find another peer with the desired file, the file transfer takes place directly through the two peers and does not pass through the supernode. FastTrack technology is used by file sharing networks including KaZazA and Grokster. For more on FastTrack, *see Morpheus Out of the Underworld,* The O'Reilly Network (July 2, 2001), *available at* http://www.openp2p.com/lpt/a/p2p/2001/07/02/morpheus.html (last visited Mar. 14, 2002).

As of October 2001, the RIAA brought a lawsuit against KaZaza, Morpheus and Grokster. Since these P2P networks are operated by a series of individuals, not by a central Web site or company, the only way to shut such networks down is one user at a time. Because those users can be anywhere in the world, that's a near-impossible task. The outcome of this suit will likely answer some of the critical questions posed by the current "copyright crisis," but the question of how a potential injunction will be enforced still remains.

168. Many believe that the idea of copyright is outmoded and that the current laws do not apply anymore. This idea was expressed by Freenet's Ian Clarke in the statement, "I do believe that through technology, the freedom to communicate can be guaranteed. It's certainly possible that Freenet could be banned. The question is whether that's enforceable." *See* Karlin Lillington, W*hy Copyright Laws Hurt Culture* (Nov. 27, 2001), *available at* http://www.wired.com/news/print/0,1294,48625,00.html (last visited Mar. 13, 2002).

that a particular copyright was violated under U.S. law or an international treaty, if the violator is anonymous, there is no central server in the chain of infringement and the court is powerless to stop the work's continued distribution, application of U.S. copyright law does not resolve the matter. Current copyright law may have "bark," but it has limited "bite."

The law alone will not resolve this "copyright crisis," but changes in the law are required. The onslaught of new file sharing technologies and their ubiquitous adoption by consumers is cause for broadening copyright law in the U.S. and throughout the world. Many say that copyright law, specifically the DMCA, is already too broad and lobby for its revision and a weakening of its restrictions.[169] This approach, however, would make the situation far worse than it already is. Instead, copyright law protection needs to be strengthened in two areas.

First, the doctrine of vicarious liability should be expanded for the Internet context. Traditional vicarious infringement doctrine requires control over the direct infringer and financial benefit to the third party. The two elements of control and financial benefit are lacking with many of the file sharing technologies at issue. In cases where a developer knowingly creates software with significant infringing uses, the control and financial gain factors should be waived. An ideologue such as Ian Clarke is not seeking economic benefit and systems such as Freenet, FastTrack and Gnutella have no central control. They do not fit the current structural standards for civil liability or criminal guilt under a vicarious infringement theory. Yet post-Napster file sharing developers know that their applications will be used for substantial infringing activities on a massive scale and should not escape liability so easily. Developers such as Clarke, Deep and others are creating technologies with the clear intent of allowing copyright infringement and then hide behind the doctrine of fair use arguing "substantial non-

169. The most contentious issues for those calling for a revision of the DMCA are the lack of a digital "first sale" doctrine and the lack of exemptions for temporary "incidental" copies and "back up" copies of creative works. The traditional first sale doctrine in copyright law allows a consumer to redistribute a copyrighted work that they have legally purchased. In August 2001, the U.S. Copyright office released a report to Congress finding that a digital first sale doctrine could hurt the market for original material. The Copyright office did recommend, however, that an incidental copy of a work made in the course of streaming is a legal fair use and that the DMCA be amended to allow for lawful backup copies of digital files. *See* Bill Holland, *Copyright Office Proposes Key Changes To DMCA*, BILLBOARD BULLETIN, Aug.t 30, 2001.

infringing use." Doug Isenberg, editor of gigalaw.com,[170] raised a counter argument to these defenses.

> "I don't think that it's clear from the Ninth Circuit's opinion that the defendants in that situation could avoid liability," Isenberg said, referring to creators of such file-trading applications [that are architected to avoid liability]. "I think (the defendants would have) good arguments, but I think they're unlikely to hold up under the Ninth Circuit ruling. Had the creators of [the technology] not created that particular application — by not creating it in the first place — the creators would have been able to block that copyright infringement."[171]

Where the developer knows or should have known that their software will be put to substantial infringing uses, the developer should be held liable for vicarious copyright infringement.

A corollary to broadening vicarious liability in this context is also narrowing the fair use defense. The Internet allows a single actor to distribute a copyrighted work to millions of users, across jurisdictional lines with little effort or cost. This unique context mandates a narrower fair use defense. As noted, a technology developer may be exempt from liability under a fair use defense where the software has "substantial non-infringing uses."[172] In the case of a digital application only, the standard should instead be that a fair use defense is barred where a technology has "substantial infringing uses." Though this may impede innovation to a degree and therefore impinge upon one of the core values of copyright,[173] this is outweighed by the other value of copyright, the property right.[174] There must be a balancing between the policy values. Innovation at the expense of another's rights is not the proper balance. The constitutional value of innovation should not be "innovation at all costs." A developer can innovate, but he must do so responsibly by ensuring that their new technology will not have "substantial infringing uses" by independent actors beyond their con-

170. gigalaw.com describes itself as: "an online resource for technology professionals and the lawyers that serve them."

171. *See* Declan McCullagh, *Good Gnus in Napster Ruling* (Feb. 14, 2001), *available at* http://www.wired.com/news/print/0,1294,41784,00.html (last visited Apr. 14, 2001).

172. *See supra* note 161.

173. The policy of creative innovation is a core constitutional value of copyright under Article I, §8, "To promote the Progress of Science and useful Arts."

174. Article I, § 8 of the Constitution also grants a limited property right in an author's creative expression, "by securing for limited Times to Authors and Inventors the exclusive Right to their respective Writings and Discoveries."

trol. If they do not, it does not necessarily mean they are liable for copyright infringement, but they should not get the benefit of even raising the fair use defense. Perhaps this rule would actually increase innovation. A limitation on the fair use defense might push developers to go beyond simply developing efficient ways of exchanging digital data over the Internet, but instead to create efficient ways of exchanging digital data over the Internet without infringing upon other's rights.

Although these changes in the law are potential deterrents to development of uncontrollable, substantially infringing technologies, the quickest, effective solution to widescale copyright infringement of music on the Internet is not a legal one. Technology itself is the best way to counteract uncontrollable technology. There are two technological methods of counter acting this problem. The first goes to the source of the problem by creating copy protected CD's. Copy protection makes it nearly impossible[175] to "rip" music into MP3 files from CD's and then trade the files within file sharing systems. Most copy protected CD's won't play on a computer or play with degraded sound quality, but will play in a standard CD player.[176] The problem is that the copy protected discs that record labels have released so far have had problems. Many copy protected discs will not play in car CD players, DVD players or certain brands of standard CD players. In addition, the practice of ripping tracks from CD's for personal use on a computer and for use in multi-song compilations that are later "burned" onto CD's, is very popular and is not possible with copy protected CD's because copy protection cannot discriminate between legal and illegal behavior.

This has created a strong backlash from the public and strong fair use arguments from the legal community against anti-copy technol-

175. Copy protection cannot completely prevent unauthorized copying of music. According to Princeton professor and encryption expert Edward Felten, "none of [the anti-copy technologies] prevent unauthorized distribution. All they do, at best, is make it more difficult, more time consuming to copy things. You are not putting up a barrier to prevent copying but a speed bump that will frustrate people who want to copy illegally." *See* Patricia O'Connell, *A "Speed Bump" vs. Music Copying Master cryptographer — and Code Ccracker — Edward Felten Says Technology isn't the Answer to Digital Copyright Violations* (Jan. 9, 2002), *available at* http://www.businessweek.com/bwdaily/dnflash/jan2002/nf2002019_7170.htm (last visited Mar. 15, 2002).

176. Anti-Copy technology exploits the differences between the way audio CD players and computer CD-ROM drives read the information on discs and essentially confuses CD-ROM drives into not reading the disc. For a detailed discussion of this, *See* Charles C. Mann, *First 'Napster-proof' CD Set to Burn: Country Star Charley Pride Takes Lead with Controversial Technology*, INSIDE, Mar. 27, 2001.

ogy.[177] Since consumers are accustomed to making copies of their music collection and the Audio Home Recording Act allows duplication for personal use, the fair use argument against anti-copy technology is reasonable. The amount of infringement taking place on the Internet today, however, goes far beyond fair use. Once again a balancing of policy concerns is necessary. The ability of consumers to listen to CD's on their computers is important, but does this trump a copyright owner's rights? There are reasonable arguments on both sides, but the Internet context here is the critical factor. Where one digital file can be exponentially duplicated on the Internet in a short amount of time, the balance tips toward allowing some form of copy protection. Legislative regulation of hardware and software standards for copy protection that has recently been introduced in the U.S. Congress goes too far.[178] The music companies must instead develop better anti-copy technology that prevents ripping MP3 files, but allows a user to play CD's in their home and car CD players and to copy files onto analog tape or portable MP3 players.[179] The DMCA's provision against anti-circumvention of copy protection implies that copy protection is legal. Barring all copying would clearly violate fair use, but fair use does not call for the best possible copies, the doctrine simply allows limited copying under certain circumstances. The music industry should be allowed to take advantage of copy protection technology that protects its rights in the most consumer friendly method possible.

A second and even more radical approach to solve the on-line infringement problem is "anti-piracy counter measures."[180] Under this

177. Congressman Rick Boucher of Virginia believes that record companies are "seeking to use their copyright not just to obtain fair compensation but in effect to exercise complete dominance and total control of the copyrighted work." *See* Amy Harmon, *CD Technology Stops Copies, But It Starts A Controversy*, N. Y. TIMES, Mar. 1, 2002, at C1.

178. South Carolina Senator Fritz Hollings has introduced legislation to Congress called the Security Systems Standards and Certification Act which prohibits the creation, sale or distribution of "any interactive digital device that does not include and utilize certified security technologies." Those opposing the legislation say that the standards are too interventionist, favor certain software brands over others and could become quickly obsolete as technology develops. Many agree that a solution must be found but legislative regulation may not be the answer. *See* Declan McCullagh and Robert Zarate, *House Cool To Copy Protection* (Mar. 4, 2002), *available at* http://www.wired.com/news/print/0,1294,50784,00.html (last visited Mar. 13, 2002).

179. The music industry is indeed working toward a more sophisticated form of copy protection. *See* Amy Harmon, *CD Technology Stops Copies, But It Starts A Controversy*, N. Y. TIMES, Mar. 1, 2002, at C1.

180. The subject of anti-copy counter measures could fill an entire law review journal by itself. There is only limited discussion of the topic here as to its contribution to a possible solution of on-line copyright infringement.

approach copyright owners themselves could attempt to disrupt the duplication and distribution of infringing files on a given file sharing network by using various technological methods. These include information collection, spoofing and interdiction.[181] Information collection identifies different data from a file sharing network which allows the network to be mapped. This map is essentially a snapshot of the network, identifying what files are on the network, the IP addresses of specific users, digital fingerprints of specific files and other data.

Spoofing is the practice of distributing misinformation in order to frustrate illegal file sharing. There are various methods of spoofing, but the most straightforward method is to flood a network with mislabeled files so the user does not get what they are searching for. For example, a file called "The Beatles – Yesterday" which actually contains "white noise" could be introduced and replicated throughout a network so that many of the search requests for "The Beatles" or "Yesterday" would come back with the spoof file instead of an actual music file. This practice would frustrate users and make file searching much more inefficient.

Interdiction is a method of blocking access to certain files within a file sharing network. It is accomplished in various ways, but the most effective way of blocking a file is by continually occupying the download slots on a target computer by "repeatedly requesting the same file and downloading it very slowly, essentially preventing other peers from accessing the file or sharing any other file."[182] Unlike spoofing, interdiction is the most direct technological measure a copyright owner can take because it targets and prevents specific users from distributing copyrighted works.

The three anti-piracy methods are distinct, but are most effective when implemented in concert. These methods could be very effective in severely limiting file sharing without "destroying or damaging the files themselves or the user's computer or software,"[183] but they still create significant legal and public relations problems for the record industry.[184] There are various federal and state laws that could be implicated by anti-piracy measures including privacy, computer and con-

181. *See* Bill Holland, *Govt., Tech Critics Decry RIAA Tactics* (Nov. 3, 2001), *available at* http://www.billboard.com (last visited Mar. 14, 2002).

182. *See id.*

183. *See id.*

184. *See* Bill Holland, *Govt., Tech Critics Decry RIAA Tactics* (Nov. 3, 2001), *available at* http://www.billboard.com (last visited Ma. 14, 2002); Almar Latour, *Beating Napster at Its Own Game?* (Nov. 12, 2000), *available at* http://www.zdnet.com/zdnn/stories/news/0,4586,2652781,00.html (last visited Mar. 14, 2002).

sumer protection laws[185] so the music industry must proceed carefully.[186]

Potentially more damaging than the risk of criminal or civil actions against the music industry, is the potential public backlash. One of the industry's most active demographic, young people between the ages of 12-24, are also the majority of users within the various file sharing networks.[187] The public relations fall out from offensive anti-piracy measures may have a negative impact on the industry in the short term, but allowing unabated file sharing to continue will have significant long term effects that may be more damaging. The industry must consider implementing some of these technological measures in limited circumstances to prevent continued infringement.

Finally, and most important for a long-term solution, the music industry must embrace the idea behind file sharing technology and develop legal, economic models, which benefit the artists, recording companies, technology developers and the consumer. All of the major record companies have indeed started to do this by supporting a new on-line music distribution model known as the "digital subscription service." The two leading subscription services are MusicNet and Pressplay.[188] Different consortiums of the major record companies own both services and with limited exceptions, neither includes content available on the other.[189] The newly launched subscription services[190]

185. A partial list of laws that may be implicated by anti-piracy measures include the Electronic Communications Privacy Act 18 U.S.C. 2510, the Stored Communications Act 18 U.S.C. 2701, the Computer Fraud & Abuse Act 18 U.S.C. 1030, the Federal Trade Commission Act 15 U.S.C. 45.

186. The RIAA's general counsel Cary Sherman stated "it is clear that any such measures will be lawful and will constitute a very modest response to a very serious problem." But others "are concerned that the technology amounts to blocking - a so-called denial of service - which is illegal." *See* Bill Holland, *Govt., Tech Critics Decry RIAA Tactics* (Nov. 3, 2001), *available at* http://www.billboard.com (last visited Mar. 14, 2002).

187. "Many users of Napster and comparable networks are also active buyers of music at record stores. Shutting their networks down or slowing electronic traffic by tricking people into opening spoof files might not go down well." "It would shut a network down in a hurry. But it could backfire, irritate the user and damage the reputation of the record company or recording artist involved." *See* Almar Latour, *Beating Napster at Its Own Game?*, (Nov. 12, 2000), *available at* http://www.zdnet.com/zdnn/stories/news/0,4586,2652781,00.html (last visited Mar. 14, 2002).

188. *See supra* note 93.

189. MusicNet's technology was principally developed by Real Networks and AOL and is backed by BMG, Warner Brothers, EMI and others. Pressplay's technology was developed principally by Microsoft and is backed Universal and Sony.

190. Besides the industry created MusicNet and Pressplay other subscription services currently available or about to launch include: a remade Napster, Listen.com's

have various subscription levels and service options, but most allow users to stream and download a limited number of music files in exchange for a monthly fee. There is no file sharing involved in these services. They are not peer to peer networks.

These new services launched in late 2001 and early 2002 and have not released any subscriber numbers to date. So far, the press has criticized both services for their downloading restrictions and inability to burn songs onto CD's and portable players.[191] The main critique is that the music industry is only allowing consumers to rent digital music, not own it. Once a consumer stops paying for their subscription all of the music files they have downloaded through the service are disabled. The current services clearly have to develop further and get closer to the model that Napster proved is popular among consumers. The problem for the music industry is that subscription services require a complete change in the business model and economics of the music business. For the music business to allow individual song downloads that are portable and owned by the consumer in perpetuity will require a complete shift in the way the industry conducts business. The industry will have to grapple with these major issues and the public will have to be patient. It is easy to develop a compelling on-line music service like Napster where everything is free and copyright infringement is disregarded. It is a real challenge to develop a successful service that is both legal and profitable.

V. CONCLUSION

The most logical and realistic solution to the problem of on-line copyright infringement throughout the world is not simply a legal one. To be sure a solution requires changes in the law, but a long-term solution also requires offensive technological measures and creative business ideas. Many of the proposals herein are clearly controversial, but these new file sharing technologies are also controversial and to control them requires strong legal disincentives and more limitations of consumer behavior. The hope is that these requirements will be short-term and that the best minds within the legal, technology and business communities will be able to come together to develop laws, technolo-

Rhapsody subscription service and Full Audio's subscription service backed by the radio group Clear Channel.

191. For one of many press critiques, *see* Walter S. Mossberg, *Record Labels Launch Two Feeble Services To Replace Napster*, WALL ST. J., Feb. 19, 2002, at B1.

gies and business models that serve all parties' best interests, most importantly, the public's.

Jeffrey L. Dodes