

9-1-2006

Contributory and Vicarious Copyright Infringement in Computer Software: Harming One Form of Intellectual Property by Protecting Another

Robert M. Hirning

Follow this and additional works at: <http://scholarship.kentlaw.iit.edu/ckjip>

 Part of the [Intellectual Property Law Commons](#)

Recommended Citation

Robert M. Hirning, *Contributory and Vicarious Copyright Infringement in Computer Software: Harming One Form of Intellectual Property by Protecting Another*, 6 Chi. -Kent J. Intell. Prop. 10 (2006).

Available at: <http://scholarship.kentlaw.iit.edu/ckjip/vol6/iss1/2>

This Article is brought to you for free and open access by Scholarly Commons @ IIT Chicago-Kent College of Law. It has been accepted for inclusion in Chicago-Kent Journal of Intellectual Property by an authorized editor of Scholarly Commons @ IIT Chicago-Kent College of Law. For more information, please contact dginsberg@kentlaw.iit.edu.

CONTRIBUTORY AND VICARIOUS COPYRIGHT INFRINGEMENT IN COMPUTER SOFTWARE

HARMING ONE FORM OF INTELLECTUAL PROPERTY BY PROTECTING ANOTHER

Robert M. Hirning*

Introduction

“From its beginning, the law of copyright has developed in response to significant changes in technology.”¹

Two theories of copyright infringement liability, contributory and vicarious infringement,² have undergone major changes in the last 20 years, as infringement liability has been extended to manufacturers and distributors of various consumer products. Accordingly, copyright infringement liability has become increasingly applied to various computer technologies, particularly today’s popular peer-to-peer file sharing software.³

The effect of indirect infringement liability on the development and use of these products’ underlying technology has yet to be fully determined. Today, contributory and vicarious copyright infringement are more likely to be imposed as a result of the distributor’s actions promoting infringement, rather than based on specific properties of the infringing technology. As more products exhibit significant legitimate uses in addition to potentially infringing uses, the question of legality and liability becomes increasingly important.

This note will examine the effect of imposing indirect copyright infringement liability on computer software and other abstract forms of developing technology. This examination will focus on how the traditional goals and interpretation of copyright protection conflict with the progression of computer technology development.

Part I of this note describes the background and history of the development of indirect infringement law.⁴ Part II describes how infringement liability has affected various computer technologies and seeks to extract the outstanding issues from recent Supreme Court holdings.⁵ Part III describes the specific infringement issues which arise through the use and development of software, including the legality of the popular BitTorrent software.⁶ Part IV specifically

* J.D. Candidate 2007, William Mitchell College of Law; B.S., Computer Science, North Dakota State University, 2003. The author wishes to thank Amanda for her invaluable encouragement and assistance.

¹ Sony Corp. of Am. v. Universal City Studios, Inc., 464 U.S. 417, 430 (1984).

² Contributory copyright infringement is defined as either actively inducing, causing, or materially contributing to the infringing conduct of another person, or providing the goods and means necessary to help another person infringe. BLACK’S LAW DICTIONARY 796 (8th ed. 2004). Vicarious copyright infringement, instead, is a person’s liability for an infringing act of someone else, even though that person has not directly committed an act of infringement. *Id.* at 797.

³ See *infra* Part I.D–E.

⁴ See *infra* Part I.

⁵ See *infra* Part II.

⁶ See *infra* Part III.

details the ways in which these infringement issues are encountered by different types of software developers and proposes ways in which they may be avoided.⁷ This note concludes that the expansion of indirect infringement has had unintended results for both the software industry and end users, which may require statutory intervention by Congress to resolve copyright's conflicting results.⁸

I. Background

The statutory copyright protection established by Congress⁹ does not hold a party liable for acts of infringement committed by another party.¹⁰ Rather, because of Congress' failure to prescribe an indirect infringement remedy, theories of contributory and vicarious infringement developed as common law doctrines and became the most effective methods in controlling widespread end-user infringement activity.¹¹

A. Development of Contributory and Vicarious Infringement

Contributory infringement liability first occurred in cases such as those where a promoter became liable for providing infringing music compositions to performers, even though the performers committed the infringing act.¹² Thus, the promoter became liable as a contributory infringer for intentionally inducing or encouraging another's direct infringement.¹³

Liability for contributory infringement occurs either through personal conduct encouraging or assisting the infringement or through the provision of machinery or goods facilitating the infringement.¹⁴ Contributory infringement also normally requires that the contributory infringer knowingly aid or induce the infringing act.¹⁵

Vicarious infringement liability similarly developed through famous "dance hall" cases, where courts used the theory to hold dance hall operators liable for profiting from infringing acts of hired performers.¹⁶ Such liability occurred even though the vicariously liable party may not have had actual knowledge of infringement.¹⁷

⁷ See *infra* Part IV.

⁸ See *infra* Conclusion.

⁹ Congress has been given authority to create copyright laws and prescribe the exclusive remedies for copyright infringement. U.S. CONST. art. I, § 8; *Sony Corp. of Am. v. Universal City Studios, Inc.*, 464 U.S. 417, 431 (1984).

¹⁰ Statutory copyright law only imposes liability against the party who directly infringes on the exclusive rights of the copyright owner. 17 U.S.C. § 501(a) (2006).

¹¹ *Metro-Goldwyn-Mayer Studios Inc. v. Grokster, Ltd.*, 125 S. Ct. 2764, 2776 (2005).

¹² *Gershwin Publ'g Corp. v. Columbia Artists Mgmt., Inc.*, 443 F.2d 1159, 1161-62 (2d Cir. 1971).

¹³ *Grokster*, 125 S. Ct. at 2776; see *Gershwin*, 443 F.2d at 1162.

¹⁴ *Matthew Bender & Co. v. West Publ'g Co.*, 158 F.3d 693, 706 (2d Cir. 1998).

¹⁵ *Gershwin*, 443 F.2d at 1162. See generally Romualdo P. Eclavea, Annotation, *Liability as "Vicarious" or "Contributory" Infringer Under Federal Copyright Act*, 14 A.L.R. FED. 825 (2005).

¹⁶ *Shapiro, Bernstein & Co. v. H. L. Green Co.*, 316 F.2d 304, 307 (2d Cir. 1963); see also 14 A.L.R. FED. 825, *supra* note 15, at § 3-4.

¹⁷ *Gershwin*, 443 F.2d at 1162. Even in the absence of a special relationship, vicarious liability may be imposed if the person had the ability to supervise the infringing activity, or had a direct financial interest in such activity. *Shapiro, Bernstein & Co.*, 316 F.2d at 307.

Vicarious liability simply requires that one profits from direct infringement while declining to exercise a right to stop or limit it.¹⁸ Normally, this is a higher standard to meet than contributory infringement, but in some factual situations where knowledge of the specific infringing act is lacking or incomplete, imposing liability vicariously may be the only viable theory.¹⁹

The Supreme Court itself has noted in dicta that “the lines between direct infringement, contributory infringement, and vicarious liability are not clearly drawn,” requiring the full analysis and consideration of each particular case.²⁰ Both theories are important when examining the overall scope of copyright infringement liability, and in this paper will be collectively referred to as indirect infringement liability.

B. Sony Betamax

Many cases in the 20th century examined indirect copyright infringement, often focusing on entities which facilitated the unauthorized performance of copyrighted music.²¹ The Supreme Court, however, did not examine the issue of indirect infringement liability against a product distributor until 1984 in *Sony v. Universal City Studios*.²²

Sony involved the potential infringement liability of a Betamax video cassette recorder (VCR) distributed by the Sony Corporation.²³ The home consumer of the VCR was responsible for the infringing act by using the VCR to record copyrighted television broadcasts.²⁴ Since imposition of liability on so many consumers was impracticable, two movie companies sought to halt the marketing and distribution of the popular product.²⁵

The Supreme Court held that “[t]he Copyright Act does not expressly render anyone liable for infringement committed by another.”²⁶ The distribution of products which facilitated infringement could not constitute contributory infringement if the product was “widely used for legitimate, unobjectionable purposes.”²⁷

¹⁸ *Grokster*, 125 S. Ct. at 2776 (citing *Shapiro, Bernstein & Co.*, 316 F.2d at 307).

¹⁹ *Shapiro, Bernstein & Co.*, 316 F.2d at 307. However, some exceptions may exist to impose liability for contributory infringement, even in the absence of knowledge of the infringing act. *See infra* Part II.B.1.

²⁰ *Sony Corp. of Am. v. Universal City Studios, Inc.*, 464 U.S. 417, 435 n.17 (1984).

²¹ *See id.* at 438 n.18 (listing notable contributory and vicarious liability infringement cases).

²² *See id.* at 417. The majority in *Sony* noted that attempting the imposition of liability on a product distributor was “unprecedented” and a “novel theory of law.” *Cf. id.* at 457 (Blackmun, J., dissenting) (alleging that infringement claims in *Sony* were similar to many other copyright cases).

²³ Betamax was produced by Sony, and was the first widely-adopted consumer video recording system. *See* Wikipedia, Betamax, <http://en.wikipedia.org/wiki/Betamax> (last visited Jan. 30, 2006). The competing format of the VHS video cassette recorder eventually became more popular with consumers, leading to the demise of the Betamax format. *Id.*

²⁴ *Sony*, 464 U.S. at 420.

²⁵ *Id.* By the time of the *Sony* decision, Sony had manufactured and distributed millions of Betamax video cassette recorders. *Id.* at 422.

²⁶ *Id.* at 434; *see also* 17 U.S.C. § 501(a) (2006) (imposing statutory infringement liability only on persons who directly infringe copyrighted works).

²⁷ *Sony*, 464 U.S. at 442. *Sony* only examined contributory infringement liability, as a vicarious liability theory was outright rejected. *See id.* at 439.

The Court held that the primary use of the Betamax VCR, recording television programs to replay later, was a legitimate fair use.²⁸ Whether the amount of legitimate use was “substantial,” however, was questionable.²⁹ Nonetheless, the Court seemed to establish an appreciable standard of preventing distributor liability for many potentially infringing products.

C. Computer Networks and Infringement

Just as consumers’ television-watching habits challenged copyright infringement law, the propagation of the personal computer also provided an opportunity for home users to abuse copyrighted digital works. Through the rise of computer networks and the Internet, millions of users began to easily and inexpensively exchange digital files of copyrighted pictures, music, movies, and software.³⁰

Early litigation involving network operators’ liability for users’ infringing acts did not seem to establish clear standards. Some courts imposed contributory infringement liability even though network operators lacked direct control of their users’ activities.³¹ The more likely result, however, was allowing network operators to escape liability if they had no notice of infringement. The developing law recognized that a network which merely enabled users to infringe copyrights was conceptually similar to an owner of a copying machine letting the public make copies with it.³²

Based on this standard, Congress modified the Copyright Act in 1998 to specifically exempt Internet service providers from infringement liability, provided that specific steps were taken by the service provider to stop and identify the infringement.³³ This exemption, however, only applied to digital communication services, and not necessarily the underlying software technology which enabled the infringement.³⁴

D. Napster and File Sharing Technologies

²⁸ *Id.* at 456.

²⁹ Only an estimated 9% of Betamax recordings were programming authorized by the copyright holder to be recorded. *Metro-Goldwyn-Mayer Studios, Inc. v. Grokster, Ltd.*, 125 S. Ct. 2764, 2788 (2005) (Breyer, J., concurring).

³⁰ Sharing of copyrighted materials through computer networks occurred long before the introduction of the World Wide Web and standalone computer software programs such as Napster. *See* M. David Dobbins, *Computer Bulletin Board Operator Liability for Users’ Infringing Acts*, 94 MICH. L. REV. 217, 218–19 (1995); *Sega Enters., Ltd. v. Maphia*, 857 F. Supp. 679, 687 (N.D.Cal. 1994) (finding online bulletin board operator liable for infringement by allowing distribution of computer games).

³¹ *See* *Sega*, 857 F. Supp. at 686–87; *Playboy Enters., Inc. v. Frena*, 839 F. Supp. 1552, 1555–56 (M.D.Fla. 1993) (copyright and trademark infringement liability imposed on computer bulletin board operator who hosted copyright holder’s pictures).

³² *Religious Tech. Ctr. v. Netcom On-Line Comm’n Servs., Inc.*, 907 F. Supp. 1361, 1369 (N.D.Cal. 1995). The online service in this case continued to allow a user use its network after being notified of infringing activities, which subjected the service to potential contributory infringement liability. *Id.* at 1373. The service argued, unsuccessfully, that it should receive a complete exemption from liability since it was a “common carrier that merely acts as a passive conduit for information.” *Id.* at 1369 n.12.

³³ 17 U.S.C. § 512 (2006).

³⁴ *Id.* at § 512(k)(1).

The availability of infringing content did not explode until the late 1990s, when programs were specifically developed to share and download digital media files. One of the first popular file sharing programs, Napster, was a stand-alone software program which allowed users to find and download copies of popular music, shared by other users.³⁵ Such technology became dubbed a “peer-to-peer” network, due to the individual users being responsible for exchanging files between themselves on the network.³⁶

Music recording companies quickly challenged Napster with a contributory and vicarious liability infringement action, resulting in an injunction to shut down the service.³⁷ Napster’s claims that the system was capable of non-infringing use were rejected,³⁸ as were claims that online music sharing was fair use.³⁹

Music and movie copyright holders also challenged other popular online file sharing services which appeared after Napster was shut down, leading many software distributors to settle claims rather than fight lawsuits.⁴⁰ The music and movie industry even instigated direct infringement actions against home users, hoping to reduce end users’ copyright infringement.⁴¹

E. MGM v. Grokster

Although most file sharing programs clearly were liable for indirect copyright infringement, *Napster* raised the question of whether the mere existence or prominence of a product’s non-infringing uses could be sufficient to protect a software distributor from indirect infringement liability. This question became a key issue in *Grokster*,⁴² a case which reached the Supreme Court in 2005.

Shortly after Napster shut down, Grokster distributed and marketed its free peer-to-peer file sharing program.⁴³ Grokster’s technology was different in that the Grokster company did not

³⁵ *A&M Records, Inc. v. Napster, Inc.*, 239 F.3d 1004, 1011 (9th Cir. 2001). Computer software technology was available to allow the conversion of a digital compact disc music track into a compressed digital MP3 file, which then could be copied to other users. *Id.* This created the potential for one user with a legitimate copy to distribute an unlimited number of copies to the entire peer-to-peer network. *Id.*

³⁶ *Id.* Napster’s MusicShare software technology worked by having the main Napster computer servers maintain an index of the available media of online Napster users, allowing users to quickly search and locate the desired media to download. *Id.* As of 2005, the service operating under the Napster brand name is a subscription music service, allowing users to legally purchase and download copyrighted music that contains digital copyright protection. *See* Napster, <http://www.napster.com> (last visited Jan. 30, 2006).

³⁷ *A&M Records, Inc. v. Napster, Inc.*, 114 F. Supp. 2d 896, 927 (N.D.Cal. 2000), *aff’d in part and rev’d in part*, 239 F.3d 1004 (9th Cir. 2001).

³⁸ *A&M Records*, 239 F.3d at 1021. The court found that regardless of the number of infringing versus non-infringing uses of its service, Napster materially contributed to direct infringement through its “site and facilities.” *Id.* at 1022.

³⁹ *Id.* at 1015–16.

⁴⁰ *See, e.g.*, *Audiogalaxy Settles Music Piracy Lawsuit*, WALL ST. J., June 18, 2002, at D6.

⁴¹ Amy Harmon, *The Price of Music: 261 Lawsuits Filed On Music Sharing*, N.Y. TIMES, Sept. 9, 2003, at A1; *Record Industry Sues More Music Swappers*, N.Y. TIMES, May 25, 2004, at C11.

⁴² *Metro-Goldwyn-Mayer Studios Inc. v. Grokster, Ltd.*, 125 S. Ct. 2764, 2777–78 (2005).

⁴³ *Id.* at 2770.

actively facilitate user downloads.⁴⁴ Rather, users of Grokster technology were solely responsible for adding, searching, and distributing digital content, through use of the Grokster software.⁴⁵

Grokster's defense was twofold. Grokster not only alleged that its software was capable of substantial non-infringing uses, but also that it did not have any specific knowledge of users' infringing activity due to the decentralized nature of the file sharing network.⁴⁶ The Ninth Circuit agreed, believing that *Sony* stood for the proposition that liability would not be possible for a product capable of substantial non-infringing uses unless the distributor had actual knowledge of specific instances of infringement and failed to act on that knowledge.⁴⁷

The Supreme Court overruled, finding that Grokster's advertising and business actions directly fostered copyright infringement.⁴⁸ The Court held that even with evidence of substantial non-infringing use, "one who distributes a device with the object of promoting its use to infringe copyright . . . is liable for the resulting acts of infringement by third parties."⁴⁹

The unanimous *Grokster* decision was reached due to Grokster's conduct in attracting and encouraging users to infringe copyrighted materials, as the court found substantial evidence that Grokster's actions induced the end users' infringement.⁵⁰ What the justices disagreed on, and what remains unclear in current case law, is how *Sony* should be applied to products passively allowing infringement, and to what extent non-infringing uses need to exist or be prominently featured in order to be protected by the *Sony* safe harbor.⁵¹

II. Imposition of Liability on Software Creators and Distributors

A. Software and Copyright Infringement

Popular products facilitating copyright infringement, such as the Betamax VCR and the Xerox copy machine, might be considered in their own separate category of technical innovations.⁵² The creators of these products were large companies, investing many resources into developing and marketing such products. In contrast, software has progressively become

⁴⁴ *Id.* at 2771.

⁴⁵ *Id.* Grokster used a decentralized network technology, in which the users of the software contact other user "nodes" on the network, which sends the file request further down the network until the file is found. *Id.* Such technical details of the Grokster network are unlike Napster's centralized service, *see supra* note 36.

⁴⁶ *Grokster*, 125 S. Ct. at 2774–75. The total amount of non-copyrighted works on the Grokster network, or works known to be in the public domain, was estimated to be less than ten percent. *Id.* at 2772.

⁴⁷ *Metro-Goldwyn-Mayer Studios, Inc. v. Grokster, Ltd.*, 380 F.3d 1154, 1161 (9th Cir. 2004), *vacated*, 125 S. Ct. 2764.

⁴⁸ *Grokster*, 125 S. Ct. at 2780–81.

⁴⁹ *Id.* at 2778–79. The Court compared such reasoning with an exemption found in the Patent statutes, where that liability is not exempted from those who distribute a staple article of commerce if they induce patent infringement. *Id.* at 2779 n.10; *see* 35 U.S.C. § 271(b) (2006) ("Whoever actively induces infringement of a patent shall be liable as an infringer.").

⁵⁰ *Id.* at 2782. Grokster specifically marketed its service to former Napster users, even attempting to divert internet queries for Napster to its own web site. *Id.* at 2781.

⁵¹ *Compare id.* at 2783–87 (Ginsburg, J., concurring) *with id.* at 2787–96 (Breyer, J., concurring) (noting a number of differences and unresolved issues in interpreting *Sony*).

⁵² *See Metro-Goldwyn-Mayer Studios, Inc. v. Grokster, Ltd.*, 259 F. Supp. 2d 1029, 1043 (C.D.Cal. 2003) (comparing software to VCRs and copy machines).

easier to create, allowing even non-technical users to develop applications with graphical software development environments. As this accessibility to computer software development tools has increased, users have followed by creating applications which have increasingly challenged the limits of copyright law.

One reason for the overall expansion of computer software applications is abstraction, a computer science concept which allows advanced functionality to be built upon lower-level, concrete functionality.⁵³ Fourth-generation computer programming languages and development libraries have made software easier and faster to develop, while the software is able to perform more powerful and complex actions.⁵⁴

The functionality of the Internet is a good example of an abstraction. At the lowest level, electronic signals are sent over data networks.⁵⁵ At a higher level, these signals represent data that is split up into discrete pieces and sent to particular network locations.⁵⁶ At the highest level, results of downloaded data from the network are rendered in a web browser.⁵⁷ Each abstract level has its own specialized function, allowing the end product, usually the highest abstraction level, to function in the most powerful and precise way.

Abstraction found in computer programming languages has similarly made it possible for developers to easily implement theoretical concepts, such as peer-to-peer networks, without large expense or expertise.⁵⁸ Given the wide accessibility to computer technology permitting infringement, and the common availability of digital copyrighted media, it is not surprising that infringement caused by computer software has turned into a problem of staggering proportions.⁵⁹

The expansion of future computer software technology is likely to be affected by a wide variety of legal trends, especially through the development of indirect copyright infringement liability. Copyright holders cannot efficiently stop millions of infringers by filing individual legal actions. Instead, their only chance of success is to directly stop the products facilitating infringement.⁶⁰

To understand how copyright infringement liability will have an effect on future software development and associated abstraction technologies, it is important to first carefully examine what changes, if any, the Supreme Court has enumerated in its recent *Grokster* decision.

⁵³ See generally Harold Abelson et al., *Structure and Interpretation of Computer Programs* (2d ed. 1996), available at <http://mitpress.mit.edu/sicp/full-text/book/book-Z-H-10.html>.

⁵⁴ See *id.*

⁵⁵ See generally LILLIAN GOLENIOWSKI, *TELECOMMUNICATION ESSENTIALS* (2001) (describing how electronic telecommunication networks are operated).

⁵⁶ For a technical analysis of how internet data is structured and sent between networks, see Russ Schuler, *How does the Internet Work*, http://www.theshulers.com/whitepapers/internet_whitepaper.html (last visited Jan. 31, 2006).

⁵⁷ See *id.*

⁵⁸ The developer of the original version of Napster, Shawn Fanning, was a 19-year-old freshman at a university when he created a simple program to search and index music files. Brad King, *The Day the Napster Died*, *Wired News* (May 15, 2002), <http://www.wired.com/news/mp3/0,1285,52540,00.html>. The program's popularity spread primarily through its users' word-of-mouth. *Id.*

⁵⁹ See *Metro-Goldwyn-Mayer Studios, Inc. v. Grokster, Ltd.*, 125 S. Ct. 2764, 2772 (2005). Over 100 million copies of Grokster's software were known to be downloaded. *Id.*

⁶⁰ *Id.* at 2776.

B. Unanswered Questions After *Grokster*

While *Grokster* seemed to be a clear victory for copyright holders, the Supreme Court deliberately left a number of unanswered questions relevant to indirect infringement liability. First, the Court did not clarify what specific role knowledge of unlawful uses has in imposing infringement liability.⁶¹ It also did not explain to what extent vicarious liability can or should be imposed, even with regard to a third party's clearly infringing acts.⁶² Most importantly, the Court failed to clearly state when *Sony* could be applied to infringement-enabling software, leaving an open question of when a product would be found with *enough* non-infringing uses to mitigate any user infringement.⁶³

1. Is Knowledge Needed For Liability?

The question of whether actual knowledge of specific infringement is necessary for indirect infringement liability was debated long before *Grokster*.⁶⁴ In a case decided by the Seventh Circuit in 2003, knowledge of users' infringing actions was a critical issue of whether to impose infringement liability on the distributors of the Aimster peer-to-peer file sharing service.⁶⁵

In *Aimster*, the file sharing software employed encryption, so that it was impossible for the service to know whether or not the users were sharing copyrighted materials with each other.⁶⁶ Aimster hoped that the lack of such knowledge would at least prevent contributory infringement liability.⁶⁷ The Seventh Circuit disagreed, reasoning that when a defendant should know of direct infringement, “[w]illful blindness is knowledge.”⁶⁸

In contrast, the operators of the *Grokster* service directly became aware of infringing uses,⁶⁹ and directly encouraged its users to download copyrighted works.⁷⁰ The Supreme Court, however, did not expressly indicate how much weight knowledge of infringement should have in imposing contributory liability.⁷¹

⁶¹ *Id.* at 2778 (failing to describe the “point of balance” when liability is imposed from knowledge that unlawful use will occur).

⁶² *Id.* at 2776 n.9 (stating that there was no need to analyze the vicarious liability theory).

⁶³ *Id.* at 2778–79. The Court said that re-examination of *Sony* and the balance between protection and commerce should be left for “a day when that may be required.” *Id.* at 2779.

⁶⁴ See *Sony Corp. of Am. v. Universal City Studios, Inc.*, 464 U.S. 417, 439 (1984); *In re Aimster Copyright Litigation*, 334 F.3d 643, 650 (7th Cir. 2003).

⁶⁵ *Aimster*, 334 F.3d at 650.

⁶⁶ *Id.*

⁶⁷ *Id.*

⁶⁸ *Id.*

⁶⁹ *Metro-Goldwyn-Mayer Studios Inc. v. Grokster, Ltd.*, 125 S. Ct. 2764, 2772 (2005).

⁷⁰ *Id.*

⁷¹ The Court primarily looked at other factors, such as its marketing to users, and its failure to stop copyrighted content sharing, to impute intent. *Id.* at 2772. Cf. *Monotype Imaging, Inc. v. Bitstream, Inc.*, 376 F. Supp. 2d 877, 886–87 (N.D.Ill. 2005) (holding that liability could not be imposed without proof of direct infringement and distributor's knowledge of this infringement).

It has become clearer that knowledge of direct infringement is not by itself sufficient to impose contributory infringement liability,⁷² but it may help demonstrate the intent to distribute an infringing product. Thus, the unanswered question is, what degree of knowledge, combined with a lack of action to stop infringement, demonstrates clear intent to induce infringement? Would discovering an Internet review of the software showing an infringing use be sufficient? What about encouraging users to try out new file trading features? Or would unsolicited email from users, indicating that they primarily use the product for infringement, be sufficient?⁷³

Placing any weight on the knowledge of users' infringement may be misguided. Once software is released into the public sphere, it can be copied and executed an unlimited number of times. Thus, it seems the most logical result that a distributor should not be held liable for an illegal use if the distributor no longer takes affirmative steps to distribute or facilitate operation of the program.⁷⁴

The formulation of liability in *Grokster*, imposing infringement liability based on the intent-evidencing affirmative acts of a distributor, would suggest the corresponding conclusion that without affirmative acts like continuing distribution or operating the infringing service, liability should not be imposed.⁷⁵ This may explain why the Court felt that premising liability only on "purposeful, culpable expression and conduct" would not harm legitimate commerce or discourage innovation.⁷⁶ Under such a standard, no court would reasonably impose liability for an unforeseen or unexpected use which infringes copyrights.⁷⁷

Even with the assurance that some level of infringement-inducing intent is needed, the level of requisite knowledge of infringing uses should be more precisely defined to allow software creators and developers to take adequate measures that prevent infringement and avoid liability. A system of imposing liability, after the fact, for unlikely or unknown uses may have the effect of limiting innovation by legitimate developers.⁷⁸

2. Is Vicarious Liability Applicable?

The *Grokster* decision also left a large question of whether vicarious liability should be imposed on the developer of infringing computer software. Excluding Napster, claims of

⁷² *Grokster*, 125 S. Ct. at 2780 (stating that mere knowledge of infringement would "not be enough" to subject a distributor to liability).

⁷³ In *Grokster*, the Court noted that the company received unsolicited emails on how to play copyrighted works, and responded with "guidance". *Grokster*, 125 S. Ct. at 2772. What weight can be placed on such encouragement to users, however, is unclear.

⁷⁴ *See id.* at 2780.

⁷⁵ *See id.*

⁷⁶ *Id.*

⁷⁷ *See id.* Contrast the actions taken by Grokster in purposefully marketing their software to demonstrate the availability of popular songs, "attract[ing] users of a mind to infringe." *Id.* at 2774.

⁷⁸ It is questionable what effect copyright law has on "illegitimate" software specifically developed to infringe copyrights. Current copyright law has proved unable to completely stop such unauthorized uses, but it may prevent ordinary users who use nothing but commercially released and licensed software from engaging in infringing uses.

vicarious liability have not been successful in past peer-to-peer software litigation⁷⁹ and were not even considered by the Supreme Court in *Grokster*.⁸⁰

One reason why vicarious liability might be preferred over a contributory liability theory is because traditionally the law did not require actual knowledge of the infringement.⁸¹ The only substantive requirement is that the vicarious infringer profits from the infringement and fails to stop it.⁸²

Vicarious liability for indirect copyright infringement may no longer be an attractive or necessary theory for parties to plead, however, as contributory infringement law has continued to become broader and much more well-defined. In some factual scenarios, contributory infringement liability can be justifiably imposed on a party even without the knowledge of users' specific infringing acts.⁸³ And, based on *Grokster's* new formulation of imposing contributory liability when the software creator clearly intends infringement,⁸⁴ there are probably no cases where profiting from infringement will not meet *Grokster's* inducement standard.

From *Grokster's* result, it is the author's suggestion that the separate elements of contributory and vicarious infringement have become encapsulated in a single indirect infringement liability theory, while courts continue to refer to this theory as "contributory." Such a result might be viewed as a broader rejection of applying vicarious liability principles to software developers, but it is more likely that the Court, for convenience, intended to apply its similar legal concepts in one pronouncement of contributory copyright infringement.⁸⁵

The simplification of the infringement liability theory will hopefully give legitimate developers a clearer standard of how to avoid liability, and give media rights holders more effective ways of establishing liability. Having a single theory for contributory and vicarious liability, however, is unlikely to have any effect on borderline cases where a product's uses lie between clearly infringing and exclusively legitimate.

3. Is Sony a Viable Defense for Infringement-Enabling Software?

The most controversial issue presented to the Court in *Grokster* was the one which the court ignored: whether the "substantial non-infringing uses" safe harbor in *Sony*⁸⁶ could ever be applied to products like *Grokster's* peer-to-peer file sharing software. Both of *Grokster's* parties and a number of *amici curae* argued that defining what a significant non-infringing use is would

⁷⁹ Compare *A&M Records, Inc. v. Napster, Inc.*, 239 F.3d 1004, 1023 (9th Cir. 2001) with *In re Aimster Copyright Litigation*, 334 F.3d 643, 654 (7th Cir. 2003).

⁸⁰ *Grokster*, 125 S. Ct. at 2776 n.9. The Ninth Circuit held against vicarious liability because *Grokster* did not monitor or control the use of the software. *Metro-Goldwyn-Mayer Studios, Inc. v. Grokster Ltd.*, 380 F.3d 1154, 1165 (9th Cir. 2004), *vacated*, 125 S. Ct. 2764.

⁸¹ *Gershwin Publ'g Corp. v. Columbia Artists Mgmt., Inc.*, 443 F.2d 1159, 1162 (2d Cir. 1971).

⁸² *Grokster*, 125 S. Ct. at 2776.

⁸³ See *supra* II.B.1.

⁸⁴ *Grokster*, 125 S. Ct. at 2780.

⁸⁵ Cf. *Telerate Systems, Inc. v. Caro*, 689 F. Supp. 221, 228 n.8 (S.D.N.Y. 1988) ("The theory of vicarious liability in the context of intellectual property is alternatively called 'contributory infringement'").

⁸⁶ See *Sony Corp. of Am. v. Universal City Studios, Inc.*, 464 U.S. 417, 442 (1984).

determine whether Grokster would be liable.⁸⁷ The Court, instead, bypassed all issues of non-infringing use by imposing liability based on Grokster's intent to produce an infringing product.⁸⁸

The result of the Court's ignoring of the non-infringing use issue seems to create a large gap between the uses found legitimate in *Sony* and the clearly infringing uses in *Grokster*.⁸⁹ It is up to future litigation to determine how to apply *Sony* in such borderline cases, but the concurring opinions by Justices Ginsburg and Breyer give some indication of how courts may approach this issue.

Justice Ginsburg argued that the *Sony* safe harbor should be strictly construed, requiring Grokster to demonstrate, "beyond genuine debate," a reasonable prospect that substantial non-infringing uses were likely to develop in the future.⁹⁰ Justice Breyer countered with a number of examples of the non-infringing use of the Grokster software, suggesting that the mere *capability* of substantial non-infringing use would be sufficient to invoke the *Sony* safe harbor.⁹¹

The majority opinion did give limited support for the *Sony* safe harbor, stating that *Sony* struck "a balance between the interests of protection and innovation."⁹² Similarly, the majority viewed its imposition of the inducement rule as "do[ing] nothing to compromise legitimate commerce or discourage innovation having a lawful promise."⁹³

Perhaps *Sony's* safe harbor is not any sort of testable standard, but instead is an encouragement for courts to do detailed fact-finding of whether the product in question has such a lawful promise. This fact-finding process would certainly be very subjective and might err repeatedly in favor of copyright holders.

The best result for the development of computer software and other technology products would be to move beyond a subjective measure of future uses, to some sort of rule-based standard which can be measured in current terms. Manufacturers of technology may not know or appreciate all of their products' current uses, much less be able to accurately predict whether the product will have *substantial* non-infringing uses in the future.

Without a solid affirmation that *Sony* will be applied to novel and groundbreaking technology products, it is likely that some commercial developers will not take the risk of releasing potentially infringing innovations. Even more troubling to all software developers, however, is the prospect that infringement liability might apply not only to software applications, but to underlying software technology as well.

III. Infringement From Underlying Computer Technology

⁸⁷ See *Grokster*, 125 S. Ct. at 2778.

⁸⁸ *Id.* at 2780.

⁸⁹ See Robert A. Kalinsky & Gregory A. Sebald, *Intellectual Property Today*, at 12 (Aug. 2005).

⁹⁰ *Grokster*, 125 S. Ct. at 2786.

⁹¹ *Id.* at 2790.

⁹² *Id.* at 2782; see also *id.* at 2781 n.12.

⁹³ *Id.* at 2780.

In the wake of the *Grokster* decision, it is clear that technology which is specifically designed or marketed to facilitate copyright infringement will subject its creator or distributor to contributory infringement liability.⁹⁴ What is unclear from any case law, however, is whether liability can be imposed based on the underlying technology facilitating the infringement.

A. Decentralized Networks

While the file sharing program in *Grokster* was found to induce its users' infringement,⁹⁵ it is questionable what role the underlying decentralized network technology had on the Court's decision. Decentralized networks pose a unique legal challenge due to their independence and lack of control once publicly released by their software creators.⁹⁶

One reason cited for imposing liability is that through the creation and distribution of decentralized network software, the creator has materially contributed to the infringement.⁹⁷ It is true that without the software creator, the infringement would never have occurred, but liability should not be imposed solely on a cause-in-fact argument. If anything, *Grokster* reinforced the proposition that a distributor needs to be directly responsible for a certain level of infringement-inducing fault before being held responsible for users' copyright infringement.⁹⁸

Similarly, contributory copyright infringement seems very hard to impose on the creator of decentralized network software due to the inability of its creator to have specific knowledge of infringement.⁹⁹ However, various methods of hiding knowledge, such as encrypting the users' activities, probably cannot be viewed as a legitimate way to prevent knowledge of infringement.¹⁰⁰

Even if a software creator originally intended or designed a product for solely legitimate uses, it is unclear whether courts would respect such a motive if the software easily allows the user to infringe.¹⁰¹ Again, asking whether copyright infringement liability would be imposed for such a product may be a restatement of *Grokster*'s unanswered questions, namely what constitutes a material contribution to infringement, and what level of knowledge of infringement is needed.¹⁰²

⁹⁴ *Id.*

⁹⁵ *Id.* at 2782.

⁹⁶ See generally Wayne Carroll, *I Want My MP3: Secondary Copyright Liability In A Hidden Peer-To-Peer Network*, 5 J. HIGH TECH. L. 235 (2005) (discussing the history of various peer-to-peer decentralized networks, including Gnutella, Grokster, and Freenet).

⁹⁷ See Matthew J. Rust, Casenote, *Nobody Uses Betamax Anymore And Neither Should The Supreme Court*, 28 HAMLINE L. REV. 549, 579 (2005).

⁹⁸ See *Grokster*, 125 S. Ct. at 2780.

⁹⁹ The argument that liability should not be imposed due to the lack of specific knowledge of users' infringement was made unsuccessfully in *Grokster*, but it may have been disregarded because of *Grokster*'s infringement-inducing acts. *Id.* at 2778.

¹⁰⁰ See, e.g., *In re Aimster Copyright Litigation*, 334 F.3d 643, 650–51 (7th Cir. 2003).

¹⁰¹ One decentralized network, Freenet, promotes itself as a "free speech" tool, rather than as a file sharing service. See Ian Clarke, *The Philosophy behind Freenet*, <http://freenet.sourceforge.net/index.php?page=philosophy> (last visited Jan. 30, 2006).

¹⁰² See *supra* Part II.B.1 (discussing requisite level of knowledge needed to impose liability).

As new uses for Internet technologies emerge, additional legitimate uses for decentralized networks are likely to be invented and utilized. Once this occurs, legal protection will likely be extended to the underlying decentralized technology, provided that its use is consistent with the results in *Sony* and *Grokster*. Of course, the creators of decentralized networks argue that legitimate uses for their technology already exist and are in widespread use today.

B. BitTorrent: Legal or Infringing?

A good example of a decentralized network which has a large potential for legitimate use is BitTorrent. BitTorrent software was originally designed to efficiently facilitate large file transfers over its decentralized network by having more of its network users participate in data distribution.¹⁰³ The main use of BitTorrent, however, has developed into the distribution of copyrighted music and movie files.¹⁰⁴

Defenders of BitTorrent technology point out major differences between it and other peer-to-peer technologies.¹⁰⁵ First, unlike many decentralized networks, BitTorrent technology by itself does not offer a search utility to find content; instead, a user wishing to download any content must manually find a source from which to download.¹⁰⁶

Second, BitTorrent technology has the capability to show the host who is providing the copyrighted content, giving copyright holders and Internet service providers an easier opportunity to identify and shut down infringers.¹⁰⁷ Increased success in stopping such infringement is unlikely, due to the costs of identifying infringement and the increasing popularity of BitTorrent.¹⁰⁸ In 2005, files traded with BitTorrent allegedly made up 30 percent of all Internet data traffic.¹⁰⁹

The best argument for not imposing infringement liability on BitTorrent is the same reason it facilitates a large amount of infringement: because it is an inexpensive technology for

¹⁰³ BitTorrent, What is BitTorrent?, <http://www.bittorrent.com/introduction.html> (last visited Jan. 30, 2006). BitTorrent, like all peer-to-peer networks, does not use a single source to spread data to many clients. Clive Thompson, *The BitTorrent Effect*, *Wired Magazine* (Jan. 2005), available at <http://www.wired.com/wired/archive/13.01/bittorrent.html>. Instead, the clients themselves help the distribution, taking advantage of the grid attributes of computer networks. *See id.* BitTorrent allows even more efficient data distribution, because each user participates in the distribution, even while they are downloading. *See id.*

¹⁰⁴ The BitTorrent Effect, *supra* note 103. Because the typical size of a video file is hundreds or thousands of times larger than a MP3 music file, it would take hours for the average home user to download a video file. *Id.* However, the BitTorrent network reduces single-source downloading bottlenecks by maximizing download and upload capability from multiple sources, allowing short videos like television shows to be downloaded in minutes. *See id.*

¹⁰⁵ *See* Wikipedia, BitTorrent, at <http://en.wikipedia.org/wiki/Bittorrent> (last visited Jan. 30, 2006).

¹⁰⁶ While the BitTorrent software itself does not provide a mechanism to find copyrighted content, the BitTorrent website provides a search box to search available content, and can easily find many copyrighted files. *See* BitTorrent, <http://www.bittorrent.com> (last visited Jan. 30, 2006).

¹⁰⁷ Wikipedia BitTorrent, *supra* note 105.

¹⁰⁸ *See generally* Gregory Scott Nortman, Indirect Liability of ISPs for Peer-To-Peer Copyright Infringement After the Verizon Decision, 7 TUL. J. TECH. & INTELL. PROP. 249, 256–59 (2005) (discussing the challenges decentralized networks pose for Internet Service Providers).

¹⁰⁹ *EDonkey packs a wallop in file sharing*, ST. LOUIS POST-DISPATCH, Sept. 9, 2005, at C6. By July 2005, a similar decentralized network named EDonkey became more widely used than BitTorrent. *Id.*

distributing large amounts of data that may or may not be infringing.¹¹⁰ Neither peer-to-peer nor centralized file distribution technologies can distribute data as effectively, and BitTorrent certainly has the potential for substantial non-infringing uses.¹¹¹

It is imperative that BitTorrent not be legally viewed as a simple peer-to-peer file sharing service, but rather as an advanced technology to efficiently distribute data. Without a clear declaration that legitimate uses of such advanced technology are adequate to prevent indirect infringement liability, new software applications like BitTorrent will not be widely distributed to the public, and the full potential of such technologies will never be realized. This consequence will have the immediate effect of holding back innovative advances which can only be measured by a product's full-scale deployment among the public.

It may seem that the rights of copyright holders and the collective need for copyright protection outweighs any amount of legitimate use of BitTorrent or other decentralized networks. However, unless a more accurate way is developed to balance future non-infringing uses with the present concerns of copyright holders, harm will likely result to BitTorrent and the application of many other promising technical concepts.

C. Software Abstraction Liability

Since unrestricted technologies such as BitTorrent have such a high potential for damaging copyright infringement abuse, copyright holders will likely continue to challenge the most widely used infringing services and their creators.¹¹² Such a result will undoubtedly persuade many developers to place safeguards against infringement in their software.¹¹³

It may seem that even as infringement liability expands, the development of overall software technology will be unaffected, because commercial software developers will find ways to expand technology while preventing infringement. Thus, specific applications of potentially infringing technology may never reach the general public. Infringement liability, however, might still be imposed if these protections are bypassed, or if software is extended to a higher abstraction.

One area of concern is the imposition of liability on creators of software programming libraries, or other tools which help develop infringing applications.¹¹⁴ For instance, if a programming language contains functionality which makes it easy to create an application to

¹¹⁰ See generally, The BitTorrent Effect, *supra* note 103.

¹¹¹ E.g., current legitimate uses of BitTorrent include distribution of the free Linux operating system, software patches, and authorized movies. Wikipedia BitTorrent, *supra* note 105.

¹¹² One decentralized peer-to-peer file sharing network, LimeWire, eventually decided to take an opt-in approach to downloading, only allowing its users to download pre-approved or licensed material. Slyck News, *LimeWire Works to Block Unlicensed Material* (Sept. 25, 2005), <http://www.slyck.com/news.php?story=927>.

¹¹³ Although it undoubtedly is a wise decision to add such safeguards to software, courts are "unable" to impose contributory infringement liability on the sole basis that the developer did not add affirmative measures to prevent infringement. *Metro-Goldwyn-Mayer Studios Inc. v. Grokster, Ltd.*, 125 S. Ct. 2764, 2781 n.12 (2005).

¹¹⁴ See generally Dennis M. Kennedy, *A Primer On Open Source Licensing Legal Issues: Copyright, Copyleft, and Copyfuture*, 20 ST. LOUIS U. PUB. L. REV. 345 (2001) (contrasting types of programming methods found in open source and commercial software).

directly infringe copyrights, would liability extend to the distributor of the programming language? What if the programming language contained extensive functionality to execute an infringing peer-to-peer program, so that all the developer needed to do was develop a simple user interface?

Again, a cause-in-fact analysis might hold the developer of such programming functionality liable for contributing to the infringement, because the infringement would not have occurred without the underlying functionality. Even if the standard of liability is material contribution to the infringement, programming languages and tools would likely contain advanced functionality, without which the infringement would not occur. This reality supports placing liability on the programming language creator.

There is no current case law to support imposing liability on underlying software technology for any legal harm, copyright infringement notwithstanding. The closest analogue might be the imposition of copyright infringement liability on an Internet service provider (ISP), when its underlying technology is actively used to infringe copyrighted media.¹¹⁵

Even this example has limits, because an ISP is selling a service, and liability is being imposed for the provision of Internet service to the user, rather than the product provided through the Internet service itself. Furthermore, Congress created a statutory safe harbor for ISPs in the Digital Millennium Copyright Act (DMCA), preventing imposition of liability if ISPs assist copyright holders in stopping infringement.¹¹⁶

Similarly, the concept of imposing liability on lower abstraction levels might suggest imposing liability for the creators of lower level Internet technology, such as a new protocol directly built into the Internet framework which lends itself to infringing uses.¹¹⁷ By enacting the DMCA, however, Congress likely intended to impose liability on ISP inaction, rather than on Internet technology which facilitates infringement.¹¹⁸

Another interesting scenario might occur if a commercial program, which contains protections against being used for infringement, is modified by its users to facilitate infringement. (The exact method of modification is not important, but this scenario may give clues to where the law would impose liability.)

In this hypothetical scenario, Company A produces a widely-used music player software allowing users to legally copy music from their CDs to their own computers to create a digital library. This program contains a digital rights protection system so that the music files can only be played on the original computer and cannot be copied. Also assume that this program has the ability to see what music other users have and listen to, such as viewing a friend's playlist,

¹¹⁵ See, e.g., *Hendrickson v. eBay, Inc.*, 165 F. Supp. 2d 1082, 1087 (C.D.Cal. 2001) (addressing issue of whether internet service provider could be held liable for facilitating distribution of infringing content).

¹¹⁶ 17 U.S.C. § 512 (2006); see also *Hendrickson*, 165 F. Supp. 2d at 1088.

¹¹⁷ Techniques have been proposed to help improve network transport for certain applications, such as voice over IP service and streaming multimedia. See, e.g., Wikipedia, Quality of Service, available at http://en.wikipedia.org/wiki/Quality_of_Service (last visited Jan. 30, 2006). Similar functionality built into internet hardware and protocols might improve file sharing or other infringing activities.

¹¹⁸ See 17 U.S.C. § 512 (2006).

although at this point there is no file trading or infringement. The program contains functionality which would allow users to trade files, but it has been disabled by Company A.

If a software patch became available on the Internet such that the anti-copy and anti-trading protections became disabled, would Company A be liable, or would the creator of the patch be liable? Would it be fair to impute the entire fault on the users, since they are committing direct infringement? What if, instead of a software patch being released, the infringing functionality could be manually enabled by end users through a simple action, like editing a text file?

Congress addressed some of these scenarios in the DMCA, making it a crime to directly circumvent some copyright protection technologies or produce a circumventing tool.¹¹⁹ Liability under the DMCA is imposed on both users and distributors who circumvent a technology that “effectively controls access” to a copyrighted work,¹²⁰ whereas liability is only imposed on creators and distributors whose tools circumvent technology that “effectively protects” a copyright owner’s right.¹²¹ Thus, in the example presented, we can assume that the user of Company A’s music player has access to the copyrighted work but is prevented from redistributing copies of the copyrighted work.¹²²

If the user downloads a patch from the Internet to enable the music program to copy and trade files at will, the creator of this patch has likely violated the DMCA.¹²³ But presumably, if the user takes a simple action, like editing a text file, to copy and trade files at will, he or she has not manufactured or provided a circumvention tool to the public and has not violated the DMCA.¹²⁴ The user has committed no harm until the he or she takes some action to violate copyright law, such as by distributing this music file on the Internet. To stop Company A’s software from facilitating such infringement, the only remedy is for the copyright holder to turn to contributory and vicarious infringement,¹²⁵ as the DMCA will not apply to Company A or the end user.¹²⁶

It is probable that if the primary tool of infringement enforcement becomes imposition of indirect liability, some programmers and software developers will begin to avoid developing software which involves copyrighted media or its potential creation, storage, or distribution. This may ultimately hinder legitimate research and product development, leading to technical stagnation and a lack of incentive to develop certain types of innovative technologies. Some have

¹¹⁹ 17 U.S.C. § 1201 (2006). See generally Amy P. Bunk, Annotation, *Validity, Construction, and Application of the Digital Millennium Copyright Act*, 179 A.L.R. FED. 319 § 7 (2006) (describing the DMCA protections and exceptions for anti-circumvention technologies).

¹²⁰ 17 U.S.C. § 1201(a). One problem remains is that there is no definite standard or clear interpretation of *how* effective an access control protection needs to be in order to warrant inclusion under this section of the DMCA.

¹²¹ 17 U.S.C. § 1201(b).

¹²² This means that the “additional violations” section of the DMCA, 17 U.S.C. § 1201(b), would apply.

¹²³ 17 U.S.C. § 1201(b)(1); 17 U.S.C. § 1201(b)(2)(A). This assumes the copyright holder would have standing to bring an action under the DMCA against the patch creator.

¹²⁴ See 17 U.S.C. § 1201(b)(1).

¹²⁵ This assumes that the inducement standard in *Grokster* will not apply, because Company A would not have the requisite intent to enable or promote infringing uses. See *supra* Part I.E.

¹²⁶ The DMCA itself notes that it is not intended to “enlarge or diminish vicarious or contributory liability.” 17 U.S.C. § 1201(c)(2).

argued that studies reveal a similar chilling effect on scientific research due to the threat of patent infringement.¹²⁷

Congress might need to intervene with statutory modification if indirect infringement liability imposes measurable effects on the software industry. In the meanwhile, it is speculative to wonder to how far courts will go in imposing liability on underlying software technologies and their developers.

IV. Effects of Liability on Software Developers

Each of the main areas of industry concerned with indirect infringement liability have separate goals and aspirations for technology development. Innovative developments in the computer science field are not confined to commercial research and development; they are equally likely to arise from academic research, open source development, or even college student hobbyists.¹²⁸

A. Academic Research

Academic research of computer software serves two useful purposes not found elsewhere. First, it encourages students and researchers to formulate theoretical computer science concepts examined from academic requirements rather than those of commercial success.¹²⁹ Second, these theoretical concepts are applied to improve existing technologies often used in non-academic settings.¹³⁰ Since such improvement of software technology often involves conflict between the accessibility of and the restrictions on intellectual property, it is not surprising that academic research readily encounters indirect infringement liability issues.

In the DMCA, Congress specifically gave an exemption to educational institutions for research activities by faculty members and graduate students that would otherwise violate the anti-circumvention provisions of the DMCA.¹³¹ While the DMCA does not specifically address indirect infringement liability, it is demonstrative of Congress' intent to protect academic research and its work with potentially infringing technologies.

¹²⁷ See American Association for the Advancement of Science, Intellectual Property in the AAAS Scientific Community: A descriptive analysis of the results of a pilot survey on the effects of patenting on science, Oct. 20, 2005, <http://sippi.aaas.org/survey/Survey%20Report%20ExecSumm.pdf> (detailing result of survey showing that 40 percent of scientific researchers have encountered problems with intellectual property rights, including having work delayed, changed, or abandoned).

¹²⁸ See *supra* note 58 and accompanying text (describing how Napster was created by college student Shawn Fanning).

¹²⁹ See generally Computing Research Association, *Evaluating Computer Scientists and Engineers for Promotion and Tenure*, http://www.cra.org/reports/tenure_review.html (last visited Jan. 31, 2006). Academic achievement for computer science and other academic fields is primarily recognized through publication and peer evaluation, rather than through commercial success or promotion. See *id.*

¹³⁰ See *id.* (explaining that academic research of computer science and engineering involves theory and experimentation, with the goal of establishing "better" inventions).

¹³¹ See 17 U.S.C. § 512(e) (2006) ("infringing activities shall not be attributed to the institution" if the educational institution provides copyright information to its system users and takes steps to promote compliance with copyright law).

An example of a new technology being developed in academic and private research is nanotechnology, which can reasonably be compared to today's computer software technology. Hypothetical nanotech manufacturing may eventually be able to duplicate and infringe any form of property on a molecular scale.¹³² Indirect infringement liability for both copyright and patents will certainly be a possibility once nanotechnology is able to mature to a commercially successful point.

Ideally, infringement liability should not be a concern for the academic research of nanotechnology, or any other undeveloped technology. Any concern about the infringement implications of a product should not occur until a product is widely used or released into the public sphere. Rather than taking an approach of not trying to develop infringing products, researchers should attempt to understand them as completely as possible, by receiving encouragement to apply new inventive concepts.

Researchers and creators of potential infringement-enabling products should be aware of indirect infringement liability, but they should not be convinced that mere production or even release of such a product will be enough to subject themselves to indirect infringement liability. However, academic researchers should understand the implications of *Grokster* and its encouragement to not display an infringing intent or other culpable behavior. If these precautions are taken, academic research should be able to operate without significant interference from indirect copyright liability.

B. Open Source Software

Some of the purposes of academic research can also be found in open source software. Open source software is defined as software providing access to the underlying programming source code, without significant restrictions on use or redistribution.¹³³ The goal of open source is to encourage the evolution of computer software through freely sharing information and its underlying technical knowledge.¹³⁴

Many open source programs and development projects are designed to emulate commercially available software, while implementing new technological innovations and features.¹³⁵ Open source software is even touted to promote software reliability and quality, because more programmers are given the opportunity to critique and improve the source code.¹³⁶

¹³² See Francisco Castro, *Legal and Regulatory Concerns Facing Nanotechnology*, 4 CHI.-KENT J. INTELL. PROP. 140, 144 (2004). The development and use of nanotechnology also presents a number of socio-political implications, as it has the potential to be deployed in a wide variety of industries, from medical devices to military weapons. *Id.* at 142.

¹³³ Open Source Initiative, *The Open Source Definition*, available at <http://www.opensource.org/docs/definition.php> (last visited Jan. 30, 2006). Most forms of Open Source software use a copyright-enabled license to ensure that further uses or extensions of the software provide access to the source code and the license. *See id.*

¹³⁴ *Id.*

¹³⁵ Kenneth J. Rodriguez, *Closing The Door On Open Source: Can The General Public License Save Linux and Other Open Source Software?*, 5 J. HIGH TECH. L. 403 (2005). One of the most popular open source applications is the Linux operating system, which has become widely used both in private and commercial settings. *Id.*

¹³⁶ *Id.*

Freely sharing source code and advancing technology seems a noble goal, but it exposes an indirect infringement liability problem when software can be easily designed to facilitate copyright infringement. This raises two important questions specific to open source software: Is it possible that open source developers who place un-compiled source code on the Internet can be liable if this code is launched by a user for infringing purposes? And what happens when such open source software was originally designed for substantial non-infringing uses?

Even if the open source program was specifically designed for copyright infringement or blatantly induces user infringement, liability may not be able to be imposed on any party. Many open source projects have a large number of anonymous contributors unable to be identified.¹³⁷ Most importantly, stopping distribution of the program is useless if the users have the source code and are able to re-launch the infringing service.¹³⁸

Another complexity with open source software is that the distributed code of a legitimate program might be modified by users to commit infringing acts. Similarly, copyright protections built into open source software may be easily bypassed, because the very nature of open source software prevents creators from effectively placing tamper-proof protections for digital media.¹³⁹

In each of these complications, it is likely that the inducement theory expounded upon in *Grokster*¹⁴⁰ will determine whether to hold the creators of open source software indirectly liable. However, if multiple developers are involved with designing different parts of the software, and no legal entity promotes the use of the software, liability may be impossible to impute to any particular party except the end user.

The open source community often views disclosure of programs and source code as a free speech issue.¹⁴¹ But open source cannot be given such broad protection if open source programs are used to openly destroy other forms of intellectual property. Open source software developers need to realize that taking responsibility for their work and encouraging the open source community to comply with current copyright restrictions may be the only way to prevent more burdensome future legal regulations.¹⁴²

C. Commercial Software

¹³⁷ See Ryan Roemer, *The Digital Evolution: Freenet and the Future of Copyright on the Internet*, 2002 UCLA J.L. & TECH. 5.

¹³⁸ See *id.* This exact problem may occur with the Freenet peer-to-peer software program, as the program and its source code has become so widely distributed that the distribution network could be easily re-launched, even if the Freenet developers no longer distribute the program. See *supra* note 101.

¹³⁹ Joseph Gratz, Note, *Reform in the "Brave Kingdom": Alternative Compensation Systems for Peer-To-Peer File Sharing*, 6 MINN. J.L. SCI. & TECH. 399, 413 (2004).

¹⁴⁰ See *Metro-Goldwyn-Mayer Studios Inc. v. Grokster, Ltd.*, 125 S. Ct. 2764, 2780 (2005).

¹⁴¹ See Free Software Foundation, *Free Software Definition*, <http://www.fsf.org/licensing/essays/free-sw.html> (last visited Jan 30, 2006) (“‘Free software’ is a matter of liberty, not price. To understand the concept, you should think of ‘free’ as in ‘free speech,’ not as in ‘free beer.’”). See also Clarke, *supra* note 101.

¹⁴² Open source developers are concerned with changes to copyright law, fearing any significant change because open source relies on copyright licensing models to ensure that source code stays open and redistributable. See CHRISTOPHER WOLF, *DIGITAL MILLENNIUM COPYRIGHT ACT: TEXT, HISTORY, AND CASELAW* 591 (1st ed. 2003).

Most commercial software developers need not be concerned with indirect copyright infringement, because many commercial software applications do not involve the use or handling of others' copyrighted works. This may change as digital multimedia becomes more integrated into user applications, leading commercial software developers to regularly encounter infringement issues.

The very definition of commercial software, creating software for a profit, means that developers will, at a minimum, indirectly profit from the infringing uses of their software. Similarly, the sale or distribution of software is usually sufficient to make a software creator distributor aware of its infringing uses. Because the elements of contributory or vicarious infringement can be easily proved, liability is understandably a major concern if the software deals with copyrighted works.

Even if a software distributor does not clearly induce its users' infringing acts, software companies may spend considerable resources litigating this issue.¹⁴³ Similarly, there is also concern that a product's advertising and marketing would be scrutinized in an attempt to prevent any sort of an infringing intent from being exhibited.¹⁴⁴

One way of preventing harm to the commercial software industry is to allow a safe harbor similar to that existing for ISPs under the DMCA.¹⁴⁵ Such a safe harbor would prevent imposition of liability on a software developer if the developer cooperates to stop the infringing activity, such as by stopping distribution or modifying the program.¹⁴⁶ Copyright holders may argue that such an approach would encourage developers to test the limits of liability, but the inducement approach formulated in *Grokster* should prevent the most harmful infringement-inducing behavior.

The liability issues for commercial and non-commercial software have a common link, namely the outstanding potential of substantial non-infringing uses. It should be clear that protection of substantial non-infringing uses is critical to the success and development of new technology applications, in all industry settings. Copyright holders should not view potentially infringing software technology as another means to infringe copyrights but, instead, should encourage legitimate applications of developing technology to increase media marketability. Investing in new media technologies, rather than fighting them, should have the dual result of benefiting technology and media holders, one of the main purposes of having intellectual property protection.

D. An Argument for Expanding Liability

Due to the previously discussed harms realized through imposing copyright infringement liability, it seems logical to reduce and limit liability for many computer software applications.

¹⁴³ See Kalinsky & Sebald, *supra* note 89.

¹⁴⁴ See *id.*

¹⁴⁵ See *supra* Part III.C; 17 U.S.C. § 512 (2006).

¹⁴⁶ The level of cooperation required to stop infringing uses might still place a heavy burden on software developers. For example, in the *Napster* case, the district court imposed "zero tolerance" for infringement, a standard which the Napster company was not able to meet, even after working with record companies to remove copyrighted materials. *A&M Records, Inc. v. Napster, Inc.*, 284 F.3d 1091, 1098 (9th Cir. 2002).

There may be limited circumstances, however, where the expansion of liability will prove beneficial to software creators and overall technology development.

The first argument for imposing liability is that it is necessary before copyrighted works can be safely introduced to new technology platforms. If the ultimate goal of the copyright system is to promote the useful development of the arts,¹⁴⁷ then protection should be zealously given to new digital forms of media. Protections enumerated in the DMCA to encourage digital protection technologies¹⁴⁸ are a good starting point. More involvement by Congress may be needed to ensure that copyright protection is available and effective with new media forms.

Second, relatively few contributory infringement suits have been brought against technology providers, with the exception of peer-to-peer file sharing programs.¹⁴⁹ And in most cases, these peer-to-peer programs were designed for the primary purpose of infringing copyrighted material.¹⁵⁰ The broad legal standard for indirect infringement formulated by peer-to-peer litigation may not be relevant for other types of computer software, because most software is not primarily designed to make unauthorized copies of copyrighted media. Thus, imposition of liability may not have the feared chilling effects on the development of new innovations.¹⁵¹

Finally, it is possible that imposing liability on developers for potentially infringing technologies will result in more developers taking steps to prevent infringement and liability in their own products. This will have the dual effect of preventing infringement from ever occurring and encouraging a large amount of research and development in necessary copyright-protection technologies. Both of these results will have a net positive effect on the software industry and end users.

Conclusion

From the perspective of an end user, there may not be much distinction between borrowing a VCR-recorded copy of a favorite television show from a friend and downloading the same show on a peer-to-peer network. The content is the same, and infringement probably has occurred in both cases, but current copyright law only applies indirect infringement liability to the developer of the peer-to-peer program. This result makes even less sense when some parties involved in the Internet download, such as ISPs who profit from data transmission, have an opportunity to escape liability. Instead, the developer of the peer-to-peer software program must

¹⁴⁷ See U.S. CONST. art. I, § 8; *Metro-Goldwyn-Mayer Studios Inc. v. Grokster, Ltd.*, 125 S. Ct. 2764, 2793–94 (2005) (Breyer, J., concurring).

¹⁴⁸ 17 U.S.C. § 1201(a) (2006) (enumerating anti-circumvention provisions for digital copyright protection technologies).

¹⁴⁹ *Grokster*, 125 S. Ct. at 2792 (Breyer, J., concurring) (noting that given the nature of the *Sony* rule, there is “nothing in the briefs or the record that shows that *Sony* has failed to achieve its innovation-protecting objective”).

¹⁵⁰ See, e.g., *Grokster*, 125 S. Ct. at 2764 (peer-to-peer software marketed and distributed for primary purpose of infringing copyrights); *In re Aimster Copyright Litigation*, 334 F.3d 643, 646–47 (7th Cir. 2003) (similar infringing objective exhibited in distributing peer-to-peer file sharing software).

¹⁵¹ *But see* Electronic Frontier Foundation, *Supreme Court Ruling Will Chill Technology Innovation* (June 27, 2005), http://www.eff.org/news/archives/2005_06.php (claiming that “inventors and entrepreneurs will not only bear the costs of bringing new products to market, but also the costs of lawsuits if consumers start using their products for illegal purposes”).

rely on a vague, judicially-created “substantial, non-infringing use” test that has been weakened by *Grokster*.

These contradictory results should have an underlying rational basis imposed by Congress through statutory copyright considerations rather than by an over-extension of common law liability. At the very minimum, some type of a safe harbor is needed to protect the interests of legitimate academic and commercial software developers. Such a measure is not needed to protect developers from over-zealous copyright holders, but is needed to encourage the development of increasingly demanded multimedia software and its associated creation, storage, and distribution technologies.

Congress, rather than the courts, is in a much better position to balance all parties’ underlying interests to determine which developing uses should be protected versus which uses pose too great of a risk to copyright holders. This undoubtedly will require separating the underlying abstract computing technology from rogue and infringement-inducing applications of the technology. Leaving the determination of where to draw this distinction to uncertain litigation cannot have a positive impact on any industry, especially in one as dynamic as computer software.

The most positive result for the development of computing software would find the Supreme Court ascribing to its own reasoning in *Sony* when examining the next new technology to challenge copyright law. “It may well be that Congress will take a fresh look at this new technology, just as it so often has examined other innovations in the past. But it is not our job to apply laws that have not yet been written.”¹⁵²

¹⁵² *Sony Corp. of Am. v. Universal City Studios, Inc.*, 464 U.S. 417, 456 (1984).