



TOURO UNIVERSITY
JACOB D. FUCHSBERG LAW CENTER
Where Knowledge and Values Meet

Touro Law Review

Volume 24 | Number 1

Article 6

May 2014

Copyright Law, Privacy, and Illegal File Sharing: Defeating a Defendant's Claims of Privacy Invasion

Daniel Gomez-Sanchez

Follow this and additional works at: <https://digitalcommons.tourolaw.edu/lawreview>



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

Recommended Citation

Gomez-Sanchez, Daniel (2014) "Copyright Law, Privacy, and Illegal File Sharing: Defeating a Defendant's Claims of Privacy Invasion," *Touro Law Review*. Vol. 24: No. 1, Article 6.

Available at: <https://digitalcommons.tourolaw.edu/lawreview/vol24/iss1/6>

This Comment is brought to you for free and open access by Digital Commons @ Touro Law Center. It has been accepted for inclusion in Touro Law Review by an authorized editor of Digital Commons @ Touro Law Center. For more information, please contact lross@tourolaw.edu.

Copyright Law, Privacy, and Illegal File Sharing: Defeating a Defendant's Claims of Privacy Invasion

Cover Page Footnote

24-1

COPYRIGHT LAW, PRIVACY, AND ILLEGAL FILE SHARING: DEFEATING A DEFENDANT'S CLAIMS OF PRIVACY INVASION

*Daniel Gomez-Sanchez**

This Comment addresses privacy counterclaims by defendants engaged in litigation with the Recording Industry Association of America for copyright infringement.

It is well settled that those mediums that specifically provide an avenue for the illegal file sharing of music can be held liable for contributory infringement of copyright, and this Comment provides an overview of the accepted law. Furthermore, it is also well settled that those persons, who share music over the Internet, are themselves liable for direct infringement of copyright. This Comment specifically addresses the latter topic.

The Recording Industry Association of America has brought claims of copyright infringement against direct infringers. More often than not, these claims have arisen due to the monitoring of a suspected copyright infringer's computer for "stolen files." The allegations of copyright infringement, and the facts alleged therein, gave rise to counterclaims of invasion of privacy, trespass to chattels, and violations of the Computer Fraud and Abuse Act. This Comment explains why such counterclaims of privacy invasion will not survive.

After defeating the privacy counterclaims, the Comment argues that a sound recording copyright is tangible property, which is central to defeating the privacy counterclaims. It is this last analysis that stresses the importance of a sound recording copyright and its application to the current state of the unauthorized downloading of music.

Lastly, this Comment examines how arms of government are

* B.A., John Jay College of Criminal Justice, 2005; J.D. Candidate, Touro College, Jacob D. Fuchsberg Law Center 2008. Special thanks to Professor Rena Sepowitz for all of her comments and guidance during the drafting of this Comment.

attempting to remedy the illegal downloading and uploading of copyright and the ensuing copyright infringement and concludes that further protections of copyright are necessary to protect all holders of sound recording copyrights.

TABLE OF CONTENTS

INTRODUCTION	75
I. UNAUTHORIZED DOWNLOADING OF MUSIC FACILITATES COPYRIGHT INFRINGEMENT	79
A. The Sony/Betamax Decision.....	81
B. The <i>MP3.com</i> Decision	85
C. The <i>Napster</i> Decision.....	88
D. The <i>Grokster</i> Decision	92
II. THE CURRENT STATE OF THE UNAUTHORIZED DOWNLOADING OF MUSIC AND ITS APPLICATION TO COPYRIGHT INFRINGEMENT	95
A. The RIAA's Claims Against Direct Infringers	97
B. Assertion of Privacy Rights Are Not a Viable Counterclaim for Active Copyright Infringers.....	100
1. <i>Common Law Trespass to Chattels</i>	100
2. <i>Common Law Invasion of Privacy</i>	102
3. <i>The Computer Fraud and Abuse Act</i>	105
C. Musical Recording Copyrights are Much Like Tangible Property.....	107
D. Further Showings of a Derogation of Privacy Rights	111
III. CONCLUSION.....	115

COPYRIGHT LAW, PRIVACY, AND ILLEGAL FILE SHARING: DEFEATING A DEFENDANT'S CLAIMS OF PRIVACY INVASION

INTRODUCTION

The advent of Napster¹ and its successors brought about a changed view on copyright infringement, and how copyright law should be used to restrain it. At its peak, Napster boasted 1.57 million simultaneous users.² The Recording Industry Association of America ("RIAA") reported an astronomical 2.6 billion songs were downloaded every month.³ Judicial action was immediately necessary to contain the widespread infringement of copyrights.

Copyright law, standing alone, is an ineffective means of regulating the uploading and downloading of copyrighted music that leads to the massive degradation of copyright. The limitations of the Copyright Act⁴ are apparent when copyright holders attempt to assert their paramount rights against direct infringers of copyright. Currently, the Act does not allow a copyright holder to escape liability for invasion of privacy when attempting to discover the identity of direct infringers of copyright prior to discovery in civil litigation.

¹ When it was released in 1999, Napster was the first of many peer-to-peer music sharing services which made the unauthorized downloading of music a major issue in future copyright battles. See CHRISTOPHER MITTEN, SHAWN FANNING: NAPSTER AND THE MUSIC REVOLUTION (2002) for a historical discussion of Napster and its founder.

² *Report: Napster Users Lose that Sharing Feeling*, CNN.COM, June 28, 2001, <http://archives.cnn.com/2001/TECH/internet/06/28/napster.usage/index.html>.

³ Statement of Mitch Bainwol, Chairman and CEO, Recording Indus. Ass'n of Am., Before the Permanent Subcomm. on Investigations, available at <http://www.riaa.com/newsitem.php?id=EB213DD3-EFEC-E865-7B5A-ADC3408A7004>.

⁴ 17 U.S.C.A. § 101-1332 (West 2000 & Supp. 2007) (providing statutory protection for copyrights).

This Comment will focus primarily on how the owners of copyright, using copyright and property law, can break down the walls of privacy to discover the thief hiding behind the internet protocol ("IP") address.⁵

Imagine, as the owner of a record label, that you discovered music CDs were being shared over the Internet for mass consumption. Users of file sharing software were downloading your unreleased and already-released songs by the billion every month. As the owner, you believe something must be done to combat this mass infringement of your proprietary rights.⁶ Consequently, on all copies of your CDs, you install proprietary software that tracks the movements of those songs if they are placed on a user's computer. Should a song be uploaded to the Internet, the software would alert the record label of the user's infringing activity. You also hire a private internet investigation firm to scour the peer-to-peer ("P2P") networks to discover any current infringement, and allow the firm to investigate each infringer's computer to discover whether any of your other copyrights have been infringed. Is this an invasion of privacy?

How is this situation different from placing a dog tag on a domesticated animal to identify ownership, or perhaps using distinguishing marks, such as color or shape, to determine ownership?

For example, if a person walked onto another's property, and

⁵ An IP address identifies an individual's computer on the Internet. Each IP address is unique to that user. *DICTIONARY OF COMPUTER AND INTERNET WORDS: AN A TO Z GUIDE TO HARDWARE, SOFTWARE, AND CYBERSPACE* 146 (2001).

⁶ The record company wants to protect the profitability of an unreleased/released phonorecord because the copyright exists not only in the phonorecord but in the sound recording as well. The interests of the artist are tied together with the interests of the record company because most record contracts do not allow an artist to collect royalty payments until the record label has recouped its investment.

stole a chattel from the front yard, then that person is permitted to use reasonable force to recapture the chattel.⁷ While issues of privacy are implicated, the recapture of the chattel would be justified.⁸

Can these two situations be meaningfully distinguished? For example, in the former situation, is there a reason why a person hired by the record label to search for copyright infringement could not use “reasonable force”⁹ to identify the infringer and recapture the profitability of its stolen chattel?

These measures refer generally to the Sony XCP software that was installed on music CDs distributed by the music giant.¹⁰ The software was subsequently found to open a “backdoor” on users’ computers who installed the music CD, and thus left them vulnerable to internet attacks.¹¹ Sony eventually reached a settlement, which in part, precluded any attempts to use copy control protections for two years.¹² Moreover, should Sony want to collect personal information on users, it must seek express consent.¹³ Yet, this does not preclude the employment of an end user license agreement (“EULA”), to which a user, wishing to install the CD on his or her computer, must adhere to in order to “rip” the CD. The user either agrees to the

⁷ See RESTATEMENT (SECOND) OF TORTS §§ 100-106, 260(1) (1965).

⁸ See *infra* Part II.B.

⁹ Used in this sense, “reasonable force” means the employment of investigatory tactics meant to track infringers.

¹⁰ See John Borland, *Who has the Right to Control your PC?*, CNETNEWS.COM, http://news.com.com/Who+has+the+right+to+control+your+PC/2100-1029_3-5961609.html?tag=nl.

¹¹ *Id.*

¹² Settlement Agreement *In re Sony BMG CD Technologies Litig.*, No. 1:05-cv-09575 (NRB), at 27 (S.D.N.Y. 2005), available at http://www.eff.org/IP/DRM/Sony-BMG/sony_settlement.pdf.

¹³ *Id.* at 27-28.

EULA or listens to the CD through conventional means, such as a car stereo or home entertainment center.

This Comment examines whether record companies, as holders of musical copyrights, should be allowed to invade the home of suspected direct infringers of copyright to discover evidence of such infringement.

Part I of this Comment analyzes the relevant framework that caused the furor over the degradation of proprietary rights in copyright.¹⁴ From *Sony Corp. of America v. Universal City Studios, Inc.*¹⁵ to *Metro-Goldwyn-Mayer Studios, Inc. v. Grokster, Ltd.*,¹⁶ this Comment discusses the relevant cases and illustrates how in each decision the copyright owners' rights were affected and ultimately protected by the imposition of third party liability on contributory infringers.¹⁷

Part II explores the RIAA's claims against direct infringers and addresses the claims employed by direct infringers citing an invasion of their individual privacy rights.¹⁸ Specifically, Part II focuses on the limited privacy rights of direct infringers who have flouted copyright law. Owners of sound recording copyrights are entitled to use "physical force" to protect their property during the their investigation of purported copyright infringers because sound recording copyrights are much like tangible property. Such measures allow copyright owners to safeguard the profitability and viability of their individual copyrights. Furthermore, Part II demonstrates that

¹⁴ See *infra* Part I.

¹⁵ 464 U.S. 417 (1984).

¹⁶ 545 U.S. 913 (2005).

¹⁷ See *infra* Part I.

¹⁸ See *infra* Part II.

government officials believe amendments to copyright law are needed to protect copyright holders' rights against the mass facilitation of copyright infringement.¹⁹

Finally, this Comment concludes that in order for copyrights to be protected courts should not hold copyright holders liable for trespass to chattel, invasion of privacy, or violation of the Computer Fraud and Abuse Act.²⁰

I. UNAUTHORIZED DOWNLOADING OF MUSIC FACILITATES COPYRIGHT INFRINGEMENT

The United States Constitution provides that "Congress shall have Power" to award authors and inventors exclusive control over their works for a limited period of time.²¹ This power enabled Congress to enact the Copyright Act.²² The Copyright Act defines copyright ownership, the duration of a copyright, what actions constitute copyright infringement, and the remedies for such infringement.²³ Section 106 of the Copyright Act sets forth the exclusive rights held by copyright owners.²⁴ These provisions offer the basis for actions

¹⁹ See *infra* Part II.D.

²⁰ 18 U.S.C.A. § 1030 (West 2000 & Supp. 2007). See *infra* Part III.

²¹ U.S. CONST. art. I, § 8, cl. 1 provides, in pertinent part: "The Congress shall have Power . . . To promote the Progress of Science and useful Arts, by securing for limited Times to Authors and Inventors the exclusive Right to their respective Writings and Discoveries"

²² 17 U.S.C.A. §§ 101-1332.

²³ See *generally id.*

²⁴ 17 U.S.C.A. § 106 (West 2000) states, in pertinent part:

[T]he owner of copyright . . . has the exclusive rights to do and to authorize any of the following:

(1) to reproduce the copyrighted work in copies or phonorecords

. . . .

(3) to distribute copies or phonorecords of the copyrighted work to the

against contributory infringers²⁵ and direct infringers of copyright through the unauthorized downloading of music.

It is hard to imagine that the unauthorized downloading of music does not facilitate copyright infringement. With countless types of file sharing software available for mass consumption, downloading songs by popular artists with the mere click of a mouse button has never been easier.²⁶ Yet, the fight against copyright infringement began as quickly as the file sharing technology became available.²⁷

In a series of cases, courts interpreted the rights of copyright holders as paramount to those of third party technology companies that have sought to exploit or ease the frustrations of a consumer with regard to the copyright holders' protected intellectual property.²⁸ The following cases are important because the contributory infringement holdings not only affected the entertainment industry and its consum-

public by sale or other transfer of ownership, or by rental, lease, or lending

. . . .

(6) in the case of sound recordings, to perform the copyrighted work publicly by means of a digital audio transmission.

²⁵ The Copyright Act does not have an express provision for contributory infringement, which is derived solely from case law.

²⁶ As of September 2007, there were still several functioning P2P networks available. Some examples are BitTorrent clients, LimeWire, and GUNet. In Canada, it is even easier to download copyrighted music—because it is legal. See John Borland, *Judge: File Sharing Legal in Canada*, CNETNEWS.COM, http://news.com.com/2100-1027_3-5182641.html (stating that a Canadian federal judge found that, under the law, file sharing “appeared to be legal”). See *BMG Canada Inc. v. John Doe*, [2004] F.C. 488 (Can.), for the complete decision. The Canadian decision and its impact on file-sharing cases in the United States is beyond the scope of this Comment.

²⁷ Napster became available in June of 1999. The first lawsuit against Napster began with the filing of a complaint by the RIAA in December of 1999 in the United States District Court for the Northern District of California. Jack McCarthy, *Studios Sue MP3 Startup Napster*, CNN.COM, <http://archives.cnn.com/1999/TECH/computing/12/09/napster.suit.idg/>.

²⁸ See *infra* Part I.A-D.

ers, but also implicitly stated that direct infringement will occur absent a showing of fair use.²⁹ Specifically, mass facilitation of copyright infringement was at issue in the later cases.³⁰ *Sony* was the first case in which the Supreme Court cogently analyzed the doctrine of contributory infringement and its application to copyrights. The same principles were later used in *Napster* to fend off mass infringement of copyright.³¹

A. The Sony/Betamax Decision

The *Sony* decision was the first United States Supreme Court case to analyze the doctrine of contributory infringement with respect to new technology and its impact on copyright.³² The Court based its decision on the application of copyright law to technology that afforded consumers the opportunity to copy television shows directly to videocassette.³³

The issue before the Court was whether the sale of the Betamax³⁴ recording machine violated any rights conferred by the Copyright Act on copyright holders of television programming when users videotaped copyrighted television programs.³⁵ While this issue

²⁹ See, e.g., *Sony*, 464 U.S. at 447. See also *A&M Records, Inc. v. Napster, Inc.*, 239 F.3d 1004, 1013 n.2 (9th Cir. 2001) (stating that there can be no contributory infringement claim without a finding that Napster users directly infringed copyright).

³⁰ See, e.g., *Grokster*, 545 U.S. 913.

³¹ *A&M Records, Inc. v. Napster, Inc.*, 114 F. Supp. 2d 896 (N.D. Cal. 2000), *aff'd in part, rev'd in part*, 239 F.3d 1004 (9th Cir. 2001).

³² *Sony*, 464 U.S. at 434-42.

³³ *Id.* at 420.

³⁴ The Betamax machine, which was released in 1975, was the precursor to the VCR, which was released in 1976. See ROBERT V. HUDSON, *MASS MEDIA: A CHRONOLOGICAL ENCYCLOPEDIA OF TELEVISION, RADIO, MOTION PICTURES, MAGAZINES, NEWSPAPERS, AND BOOKS IN THE UNITED STATES* 350 (1987).

³⁵ *Sony*, 464 U.S. at 420.

seemed to be straightforward, Universal's argument that Sony was engaging in contributory infringement of copyright complicated the matter.³⁶ The crux of Universal's argument was that because some individuals used the Betamax machine to record copyrighted television shows, Sony was liable in damages for providing the means to infringe copyright.³⁷ The Court rejected Universal's claim that *Kalem Co. v. Harper Bros.*³⁸ established the grounds for contributory infringement, and distinguished supplying the means to a consumer to engage in infringement and actually providing the copyrighted work.³⁹ Moreover, the Court held a contributory infringer was usually in a position to control the use of a copyrighted work, whereas Sony was not.⁴⁰

In borrowing the staple article of commerce doctrine from patent law, the Court noted that a patent holder could not assert a claim of contributory infringement if the article of commerce, although utilized for infringing uses, was also exploited for noninfringing, lawful uses.⁴¹ Thus, the Court concluded that Sony's sale of the

³⁶ *Id.* at 434 (stating the Copyright Act does not expressly hold contributory infringers liable for copyright infringement).

³⁷ *Id.* at 420. Universal's allegation becomes relevant in subsequent cases against Napster and Grokster which will be examined later in this Comment.

³⁸ 222 U.S. 55 (1911).

³⁹ The Court held that *Kalem* did not provide the "means" to hold Sony liable because it would have been an argument that "rests on a gross generalization . . ." See *Sony*, 464 U.S. at 436. The Court further stated that, in *Kalem*, not only did the producer (of an unauthorized film drama based on the copyrighted book *Ben-Hur*) supply the means for infringement, he also supplied the work. *Id.* at 435-36. Moreover, the Court noted that Sony neither had any direct contact with users of the Betamax machine, nor those who infringed copyright. *Id.* at 437-38.

⁴⁰ See *id.* at 437-38. See also *id.* at 437 n.18 (citing to several cases where a contributory infringer was in control of the use of copyrighted works). This aspect of control becomes relevant in the *Napster* decision.

⁴¹ *Id.* at 441 (quoting *Henry v. A.B. Dick Co.*, 224 U.S. 1, 48 (1912)).

Betamax could not amount to contributory infringement “if the product [was] widely used for legitimate, unobjectionable purposes.”⁴²

The question then became whether Sony’s Betamax machine was capable of substantial noninfringing uses.⁴³ Sony advanced a fair use defense⁴⁴ of private, non-commercial time-shifting in the home.⁴⁵ The time-shifting defense argued that a user of the Betamax machine should be allowed to record television shows (that were broadcasted at times when the user was unavailable to watch them) and watch the shows at a later time when the user became available.⁴⁶ The Court recognized time-shifting may enlarge the viewing audience of television programs, and that several producers of television shows authorized the use of private time-shifting.⁴⁷ Further, the Court concluded such authorized time-shifting should not choke the sale of such equipment because that equipment was used by some to make unauthorized copies of copyrighted works.⁴⁸ Furthermore, the Court noted that the plaintiffs did not represent all copyright owners, but merely a small percentage.⁴⁹

[I]n an action for *contributory* infringement against the seller of copying equipment, the copyright holder may not prevail unless the relief that he seeks affects only his programs, or unless he speaks for virtually all

⁴² *Id.* at 442.

⁴³ *Id.*

⁴⁴ The fair use defense is codified in 17 U.S.C.A. § 107 (West 2000).

⁴⁵ *See generally Sony*, 464 U.S. at 442-56. The time-shifting argument gave rise to a space-shifting argument explored by the *MP3.com* and *Napster* decisions. *See infra* Part I.B-C.

⁴⁶ *Sony*, 464 U.S. at 423.

⁴⁷ *Id.* at 443.

⁴⁸ *Id.* at 446.

⁴⁹ *Id.* at 443 (stating the plaintiffs comprised less than ten percent of the market share).

copyright holders with an interest in the outcome.⁵⁰

Next, the Court addressed the unauthorized time-shifting infringement of copyright, the application of the defense of fair use, and whether it militated against a finding of substantial noninfringing use. The Court stated that it first had to weigh the factors enumerated in section 107 of the Copyright Act to determine whether use of a copyrighted work is a fair use.⁵¹ In addressing the first three factors of section 107, the Court noted the Betamax machine was not being used for commercial purposes when applied to private use in the home.⁵² Moreover, the fact that the television shows were offered in their entirety for free on their initial broadcast did not prevent a finding of fair use when the entire work was reproduced.⁵³

In addressing the fourth fair use factor, section 107(4), the Court considered the effect of the non-commercial use of the copyrighted material on the marketplace.⁵⁴ To prove that a non-commercial use is harmful, or would adversely affect the market for a

⁵⁰ *Id.* at 446. The Court's argument here would not bar the actions in *Napster*, *MP3.com*, or *Grokster*, as all the major recording companies were seeking a judgment on the case.

⁵¹ 17 U.S.C.A. § 107 states, in pertinent part:

In determining whether the use made of a work in any particular case is a fair use the factors to be considered shall include—

- (1) the purpose and character of the use, including whether such use is of a commercial nature or is for nonprofit educational purposes;
- (2) the nature of the copyrighted work;
- (3) the amount and substantiality of the portion used in relation to the copyrighted work as a whole; and
- (4) the effect of the use upon the potential market for or value of the copyrighted work. . . .

⁵² *Sony*, 464 U.S. at 449-50.

⁵³ *Id.*

⁵⁴ *Id.* at 451.

copyrighted work, a plaintiff must show by a preponderance of the evidence “that *some* meaningful likelihood of future harm exists.”⁵⁵ If the use is for commercial gain, the likelihood of harm is presumed.⁵⁶ Citing the district court’s findings, the Supreme Court found there was no actual harm, and the plaintiffs’ fears were unfounded.⁵⁷

Ultimately, the Court found the Betamax was capable of substantial noninfringing uses, therefore Sony was not liable for contributory infringement.⁵⁸ Furthermore, the Court specifically noted a direct infringer could not be liable unless the use of copyrighted material violated an exclusive right conferred by the Copyright Act, subject, of course, to whether the infringement was fair use.⁵⁹

B. The MP3.com Decision

UMG Recordings, Inc. v. MP3.com, Inc.,⁶⁰ is the first of several cases dealing with the emergence of new technology and how copyright law, post-*Sony*, would apply to digital musical copyrights.

⁵⁵ *Id.*

⁵⁶ *Id.*

⁵⁷ *Sony*, 464 U.S. at 452-53. For example, the district court noted the Nielsen ratings would not be affected, revenues would not decrease, that there was no factual basis for the plaintiffs’ prediction that live television and movie theater audiences would decrease, and that there would be a reduction in audiences for re-runs and video rental. *Id.* at 453 nn.36-39.

⁵⁸ *Id.* at 456. The *Sony* decision also contributed to the emergence of new legal theories that became relevant in later decisions when applied to the music industry cases against MP3.com, Napster, and Grokster. For example, the arguments put forth by the music industry harkened back to the arguments used in the *Sony* decision, which is why *Sony* and its legal maxims are so important and relevant today. See EFF.org, *The Betamax Case*, <http://www.eff.org/legal/cases/betamax/> (last visited Feb. 1, 2008), for a comparison of arguments made by Universal’s counsel in *Sony*, and arguments made by MGM’s counsel in *Grokster*.

⁵⁹ *Sony*, 464 U.S. at 447.

⁶⁰ 92 F. Supp. 2d 349 (S.D.N.Y. 2000).

Although the case involved direct infringement of copyright by a technology company, the holding emphasizes a theme central to this discussion: direct infringement will not be tolerated, and those who directly infringe will be held liable.

This case turned on whether MP3.com, the defendant, could purchase tens of thousands of music CDs, “rip” them into MP3 files, place those files onto their servers, and make the music files available to its customers over the Internet.⁶¹ The case presented an interesting issue because the MP3.com customers could not access the music files unless they already owned the particular CD they wanted to access.⁶² This case, however, focused on the direct infringement liability of MP3.com rather than the consumer, because MP3.com was itself infringing those rights.⁶³

MP3.com argued fair use and, to substantiate its defense, introduced a variant of the time-shifting argument that was presented in *Sony*—space-shifting—to substantiate its defense.⁶⁴ The space-shifting argument, as presented, maintained that because the customer already owned the CD, MP3.com’s placement of those MP3 files on its servers merely eliminated one step that a consumer needed to take

⁶¹ *Id.* at 350. See also *Recording Indus. Ass’n of Am. v. Diamond Multimedia Systems Inc.*, 180 F.3d 1072, 1073-74 (9th Cir. 1999) (describing the process of converting CD recordings into MP3 files, as well as defining MP3). *Diamond* also stands for another very important proposition: portable MP3 players are not digital audio recording devices within the meaning of the Audio Home Recording Act of 1992. *Id.* at 1081. Explicit in the Ninth Circuit’s determination is that users may legally transfer MP3 files of music they converted from their own private collection, thus space-shifting, for non-commercial private use. *Id.* at 1079.

⁶² See *MP3.com* for a discussion of MP3.com’s beam-it service. *MP3.com*, 92. F. Supp. 2d at 350.

⁶³ *Id.*

⁶⁴ *Id.* at 351.

to “carry” his music collection anywhere a computer with internet access was available.⁶⁵ MP3.com asserted that, under factor one of the fair use test, unauthorized copies were being transmitted in a different medium, and therefore constituted a transformative fair use.⁶⁶ However, the court dismissed this argument as implausible because MP3.com’s inclusion of the plaintiffs’ CDs on its servers was not sufficiently transformative, amounting to nothing more than a “re-playing for [its] subscribers converted versions of the recordings it copied, without authorization, from the plaintiffs’ copyrighted CDs.”⁶⁷

In discussing the second and third factors, the court determined that the nature of the copyrighted work was neither factual nor descriptive, and that MP3.com copied the entirety of the copyrighted works.⁶⁸

Regarding the fourth factor, the court found the defendant’s activities impeded the plaintiffs’ right to license the copyrighted works for reproduction.⁶⁹ While MP3.com argued that the plaintiffs had not yet entered the new market forged by MP3.com, the court rejected this contention because a holder of a copyright’s exclusive rights flowed from the Constitution and the Copyright Act, and therefore, a copyright holder had the sole right to enter a chosen “new” market.⁷⁰ Moreover, the plaintiffs introduced licensing agreements as

⁶⁵ *Id.* at 350.

⁶⁶ *Id.* at 351.

⁶⁷ *MP3.com*, 92 F. Supp. 2d at 350.

⁶⁸ *Id.* at 351-52.

⁶⁹ *Id.* at 352. *See also* 17 U.S.C.A. § 106(1).

⁷⁰ *MP3.com*, 92 F. Supp. 2d at 352.

evidence of an entry into the new market forged by MP3.com.⁷¹

Furthermore, the *MP3.com* court rejected the argument that consumer demand for a new market dictates when infringement of copyright is permissible,⁷² reasoning that such a claim was inequitable.⁷³ Thus, a consumer with access to file-sharing software, who misappropriates the property of a copyright holder, could be held liable for infringement regardless of whether consumer demand for such software was present. At first blush, the *MP3.com* decision seems inconsistent with the *Sony* decision. However, the *MP3.com* decision dealt with a mass infringement of tens of thousands of music CDs, and a claim by all the major record companies, while *Sony* involved fewer instances of infringement, with less than ten percent of the television copyright holders bringing suit. The inconsistency can best be described as a matter of degree.

As a whole, *MP3.com* supports the view that with each decision on musical copyright infringement, courts are further eroding the barrier of privacy with respect to locating direct infringers of copyright. Such a breakdown would help identify those infringing uses of copyright, and allow for better protection of authors' rights. The *Napster*⁷⁴ decision is no different.

C. The *Napster* Decision

The Ninth Circuit's decision in *Napster* is most analogous to

⁷¹ *Id.* This is further evidenced by current formats, such as Real Rhapsody and Yahoo Music Unlimited, to which record labels have licensed copyrighted works.

⁷² *Id.*

⁷³ *Id.*

⁷⁴ See *Napster*, 239 F.3d 1004.

Sony. Napster, which introduced a new breed of copyright infringement, involved a novel technology, called P2P file sharing, that facilitated copyright infringement on a colossal scale.⁷⁵ Yet, Napster was not a true P2P network because it relied on its network servers to store the vast amounts of copyrighted works traded by its users.⁷⁶ Regardless, users were able to download their favorite MP3 song files at a rate of 2.6 billion songs per month.⁷⁷ If the average album contained ten songs, Napster users were downloading the equivalent of 260 million albums per month.

Record companies filed an action against Napster for facilitating copyright infringement.⁷⁸ Napster operated a system that permitted “the transmission and retention of sound recordings employing digital technology.”⁷⁹ The plaintiffs claimed Napster users engaged in the “reproduction and distribution of copyrighted works” in violation of the exclusive rights granted to copyright holders by section 106 of the Copyright Act.⁸⁰ The United States Court of Appeals for the Ninth Circuit agreed with the district court that downloading and uploading copyrighted works by Napster users constituted direct infringement of copyright.⁸¹

⁷⁵ For an explanation of P2P file sharing see *ENCYCLOPEDIA OF NEW MEDIA* 367-368 (2003).

⁷⁶ *Napster*, 239 F.3d at 1012.

⁷⁷ Statement of Mitch Bainwol, *supra* note 3.

⁷⁸ *A&M Records, Inc.*, 114 F. Supp. 2d at 900 (“On December 6, 1999, A & M Records and seventeen other record companies (‘record company plaintiffs’) filed a complaint . . . against Napster, Inc. . . .”).

⁷⁹ *Napster*, 239 F.3d at 1011.

⁸⁰ 17 U.S.C.A. § 106; *Id.* at 1013.

⁸¹ *Id.* at 1014 (explaining Napster users who uploaded copyrighted song files violated the plaintiffs’ distribution rights under section 106(3) of the Copyright Act, and Napster users who downloaded copyrighted song files violated plaintiffs’ reproduction rights under sec-

Napster argued that its users were engaged in fair use, and therefore could not be held to directly infringe the copyrights of the plaintiffs.⁸² The three fair use defenses advanced by Napster were: (1) sampling, (2) space-shifting, and (3) permissive distribution by recording artists.⁸³ The sampling defense contended users were making temporary copies of the copyrighted songs to determine whether to purchase the work.⁸⁴ The plaintiffs did not seek to enjoin the permissive distribution by recording artists because it was inherently noninfringing.⁸⁵

In examining Napster's first defense, that Napster users were engaged in fair use, the court examined the factors enumerated in section 107.⁸⁶ The court found Napster users were engaged in commercial use of the copyrighted works,⁸⁷ and that such downloading negatively affected the music industry.⁸⁸

The court rejected the sampling defense, noting that sampling plaintiffs' copyrighted works would deprive them of collecting royalties on authorized song samples.⁸⁹ Moreover, unlicensed sampling would deprive the copyright holder of the right to license its copy-

tion 106(1) of the Copyright Act).

⁸² *Id.*

⁸³ *Id.*

⁸⁴ *Napster*, 239 F.3d at 1014.

⁸⁵ *Id.* at 1019.

⁸⁶ *Id.* at 1014-17. *See also* 17 U.S.C.A. § 107.

⁸⁷ *Napster*, 239 F.3d at 1015 (stating repeated copying of copyrighted works is the equivalent of commercial use).

⁸⁸ *Id.* at 1016-17 (stating the effect of Napster users' constant downloading impedes the ability of record companies to sell their product, and deprives the copyright owner of the right to enter a new market).

⁸⁹ *Id.* at 1018. *See also* *BMG Music v. Gonzalez*, 430 F.3d 888, 889-91 (7th Cir. 2005) (rejecting the sampling defense).

rights for authorized sampling.⁹⁰

Finally, the court rejected the space-shifting defense. The court held that the shifting methods in *Diamond*⁹¹ and *Sony* “did not also simultaneously involve [the] distribution of the copyrighted material to the general public; the time or space-shifting of copyrighted material exposed the material only to the original user.”⁹² Moreover, in *Sony*, there were only some instances of copyright infringement by users of the Betamax,⁹³ compared to the infringement of billions of copyrighted works in *Napster*.⁹⁴

Significantly, the *Napster* court held that users of software, such as Napster, may be held liable for direct infringement of copyright.⁹⁵ While this is not surprising, it foreshadowed the impending litigation against music file sharers.⁹⁶ Though proving direct infringement by users is necessary to making out a prima facie case of contributory infringement, it was not until 2003, two years after the *Napster* decision, that the RIAA began instituting actions against unauthorized filesharers.⁹⁷ According to one source, the RIAA’s move to sue individual file sharers came as a result of two separate deci-

⁹⁰ *Napster*, 239 F.3d at 1018.

⁹¹ *Diamond* involved the question of whether the use of an MP3 player, such as Apple’s iPod, was a proper exercise of fair use when users space-shifted their music collections onto the player. See *Diamond*, 180 F.3d 1072.

⁹² *Napster*, 239 F.3d at 1019.

⁹³ *Sony*, 464 U.S. at 420.

⁹⁴ See Statement of Mitch Bainwol, *supra* note 3.

⁹⁵ See *Napster*, 239 F.3d at 1019 (indicating Napster users likely do not have a fair use defense). This holding was later used by the RIAA to institute actions against individual persons for unauthorized downloading of music. See *infra* Part II.

⁹⁶ See *infra* Part II.

⁹⁷ ELECTRONIC FRONTIER FOUNDATION, *RIAA V. THE PEOPLE: TWO YEARS LATER 2* (2005) (stating that 261 file sharers were sued on September 8, 2003), available at www.eff.org/IP/P2P/RIAAatTWO_FINAL.pdf.

sions: the Central District of California's *Grokster* decision,⁹⁸ and the District of Columbia's order⁹⁹ compelling Verizon, as an Internet Service Provider ("ISP"), to provide the RIAA with account information regarding its subscribers.¹⁰⁰ The move to sue direct infringers could hardly be questioned as the RIAA, in the course of a few months, received its worst and best decision—a decision shielding Grokster from infringement liability, and a decision allowing the RIAA to subpoena the names of individual infringers from ISPs breaking down one wall of privacy.¹⁰¹

D. The *Grokster* Decision

In *Grokster*, the United States Supreme Court addressed the following question: "[U]nder what circumstances [is] the distributor of a product capable of both lawful and unlawful use . . . liable for acts of copyright infringement by third parties using [its] product[?]"¹⁰² The critical distinction between the Napster software and the Grokster software was that Grokster did not employ servers to intercept inquiries by users of the content available on the Grokster

⁹⁸ *Metro-Goldwyn-Mayer Studios, Inc. v. Grokster, Ltd.*, 259 F. Supp. 2d 1029 (C.D. Cal. 2003), *aff'd*, 380 F.3d 1154 (9th Cir. 2004), *vacated*, 545 U.S. 913 (2005).

⁹⁹ *Recording Indus. Ass'n of Am., Inc. v. Verizon Internet Services, Inc.*, No. 03-7015, 03-7053, 2003 WL 21384617, at *1 (D.C. Cir. June 4, 2003), *rev'd*, 351 F.3d 1229 (D.C. Cir. 2003), *cert. denied*, 543 U.S. 924 (2004).

¹⁰⁰ Lisa M. Bowman, *Labels Aim Big Guns at Small File Swappers*, CNETNEWS.COM, http://news.com.com/Labels+aim+big+guns+at+small+file+swappers/2100-1027_3-1020876.html (stating the decision in *Grokster* prompted the RIAA to begin suing individuals).

¹⁰¹ *See* RIAA v. THE PEOPLE, *supra* note 97, at 3-4. While the *Verizon* decision was subsequently overturned in *Recording Indus. Ass'n of Am., Inc. v. Verizon Internet Services, Inc.*, it should not bar the RIAA from locating individual infringers. *Recording Indus. Ass'n of Am., Inc. v. Verizon Internet Services, Inc.*, 351 F.3d 1229, 1239 (D.C. Cir. 2003). *See infra* Part II.

¹⁰² *Grokster*, 545 U.S. at 918-19.

network.¹⁰³ Napster, on the other hand, used central servers to intercept users' queries and even temporarily stored transferred files on its servers.¹⁰⁴ The distinction was important to the district court and the court of appeals in *Grokster*, because the lack of a central server did not impute actual knowledge of specific infringing activity.¹⁰⁵ Yet, the Supreme Court rejected this broad interpretation of the *Sony* decision because it declined to take into account certain evidence of inducement to infringe presented by MGM.¹⁰⁶ The Court stated that *Sony* "was never meant to foreclose rules of fault-based liability derived from the common law."¹⁰⁷

Just as the *Sony* Court borrowed the staple article of commerce doctrine from patent law, the *Grokster* Court borrowed the inducement rule from patent law.¹⁰⁸ In doing so, the *Grokster* Court held, "one who distributes a device with the object of promoting its use to infringe copyright, as shown by clear expression or other affirmative steps taken to foster infringement, is liable for the resulting acts of infringement by third parties."¹⁰⁹ The Court then stated that neither mere knowledge of the product's infringement potential, nor actual infringement by users, would be sufficient to impose liability on the distributor of such technology.¹¹⁰ There must be "purposeful,

¹⁰³ *Id.* at 921-22.

¹⁰⁴ *Napster*, 239 F.3d at 1012.

¹⁰⁵ *Grokster*, 545 U.S. at 927-28, 933-34.

¹⁰⁶ *Id.* at 933-34.

¹⁰⁷ *Id.* at 934-35.

¹⁰⁸ *Id.* at 936.

¹⁰⁹ *Id.* at 936-37.

¹¹⁰ *Grokster*, 545 U.S. at 937.

culpable expression and conduct”¹¹¹

Ultimately, the Court found sufficient evidence of inducement.¹¹² The evidence demonstrated Grokster had communicated directly with Napster users concerning the ability to download copyrighted music.¹¹³ Internal documents showed the other defendant, Streamcast, hoped to attract Napster users once Napster was shut down.¹¹⁴ Advertisements touted the defendants as the successors to Napster.¹¹⁵ Furthermore, there was no evidence the defendants attempted to filter the copyrighted works.¹¹⁶

Moreover, the Court noted the inducement theory required evidence that users were directly infringing copyright. Unlike *Sony*, the *Grokster* Court observed that billions of song files were being shared every month over the defendants’ networks, and ninety percent of the files available on the networks were copyrighted works.¹¹⁷ In reversing the summary judgment decision in favor of the defendants, the Court ruled theories of secondary liability must be utilized because it may be impossible to enforce rights in copyrighted works against direct infringement.¹¹⁸ One could surmise that theories of secondary liability assist copyright holders by halting the infringement at its source, thereby preventing users from directly infringing in mass numbers. Moreover, theories of secondary liability allow

¹¹¹ *Id.*

¹¹² *Id.* at 937-38.

¹¹³ *Id.*

¹¹⁴ *Id.* at 939.

¹¹⁵ *Grokster*, 545 U.S. at 924-25.

¹¹⁶ *Id.* at 939.

¹¹⁷ *Id.* at 922-23. In *Sony*, there were only a few instances of direct infringement by users. *Sony*, 464 U.S. at 420.

¹¹⁸ *Grokster*, 545 U.S. at 929-30.

copyright holders to receive substantial damage awards from contributory infringing companies, whereas collecting from a direct infringing consumer would not provide revenue to adequately recover the profitability of its infringed copyrights.

The implicit conclusion by various courts, that the facilitation of copyright infringement by new technologies was degrading the enforcement of copyright law, has created a legal framework in which to begin breaking down the walls of privacy. Courts are now holding unauthorized music sharers liable for their individual acts of infringement without regard to privacy concerns. As long as individual file sharers continue to flout copyright law, the laws of privacy should not offer a shell of protection.

II. THE CURRENT STATE OF THE UNAUTHORIZED DOWNLOADING OF MUSIC AND ITS APPLICATION TO COPYRIGHT INFRINGEMENT

In response to *Grokster*, on September 27, 2006, the United States District Court for the Central District of California granted summary judgment in favor of the plaintiff record companies, effectively putting an end to the *Grokster* issue.¹¹⁹ Yet, at the time of the decision, the case against direct infringers had been raging for more than three years.¹²⁰

The RIAA began its investigation by gathering evidence using the same software as P2P users, and retrieving the IP addresses of

¹¹⁹ See generally *Metro-Goldwyn-Mayer Studios, Inc. v. Grokster, Ltd.*, 454 F. Supp. 2d 966 (C.D. Cal. 2006).

¹²⁰ See *RIAA v. THE PEOPLE: TWO YEARS LATER*, *supra* note 97, at 2.

those infringers.¹²¹ In order to retrieve the names and addresses of the infringers, the RIAA issued subpoenas against the users' ISPs under section 512(h) of the Copyright Act.¹²² Pursuant to the subpoena power of section 512(h), the RIAA attorneys were able to discover the identities of infringers with a mere allegation of infringement.¹²³ Verizon, however, refused to comply with a subpoena from the RIAA issued under section 512(h).¹²⁴ The RIAA subsequently brought an action to compel Verizon to comply.¹²⁵ The United States District Court for the District of Columbia rejected Verizon's contentions, and ordered it to comply with the subpoena to reveal the identities of its infringing users.¹²⁶ An order staying the decision while pending appeal was issued and subsequently vacated.¹²⁷ The decision to vacate the stay authorized the RIAA to continue its onslaught against direct infringers.

On September 8, 2003, the RIAA announced its first lawsuits against direct infringers.¹²⁸ By the time the Circuit Court of Appeals for the D.C. Circuit heard Verizon's appeal, the RIAA had issued more than 3,000 subpoenas.¹²⁹ The appellate court rejected the

¹²¹ See Bowman, *supra* note 100 (stating RIAA investigators will scan the public directories of popular P2P software).

¹²² 17 U.S.C.A. § 512(h)(1) (West 2000) states, in pertinent part: "A copyright owner . . . may request the clerk of any United States district court to issue a subpoena to a service provider for identification of an alleged infringer"

¹²³ RIAA v. THE PEOPLE: TWO YEARS LATER, *supra* note 97, at 3.

¹²⁴ *Id.*

¹²⁵ See *In re Verizon Internet Services, Inc.*, 240 F. Supp. 2d 24 (D.D.C. 2003).

¹²⁶ *Id.* at 44-45.

¹²⁷ *Verizon*, 2003 WL 21384617, at *1 (D.C. Cir. June 4, 2003).

¹²⁸ Press Release, RIAA.com, Recording Industry Begins Suing P2P File Sharers Who Illegally Offer Copyrighted Music Online (Sept. 8, 2003), available at <http://www.riaa.com/newsitem.php?id=EB213DD3-EFEC-E865-7B5A-ADC3408A7004>.

¹²⁹ RIAA v. THE PEOPLE: TWO YEARS LATER, *supra* note 97, at 5.

RIAA's power to subpoena at will, and held that under section 512(h) the power to issue subpoenas was available only where the infringing files were located on an ISP's own computer system.¹³⁰ Therefore, to continue gathering identities, the RIAA would have to file a lawsuit, and seek the names and addresses of infringers through discovery, under the supervision of a court.¹³¹

The Court of Appeals decision, however, did not deter the filing of lawsuits. By 2005, the RIAA had sued over 15,000 infringers.¹³² The RIAA's lawsuits are the focus of the following sections of this Comment.

A. The RIAA's Claims Against Direct Infringers

Collectively, the RIAA and individual record companies have filed suit against over 15,000 individuals.¹³³ The complaints largely state one claim: copyright infringement.¹³⁴ The infringement complaints focus on violations of the exclusive rights to reproduce and distribute under section 106 of the Copyright Act.¹³⁵

To present a *prima facie* case of direct copyright infringement, a plaintiff must show ownership of the copyrighted music and demonstrate a violation of at least one of the enumerated exclusive

¹³⁰ Recording Indus. Ass'n of Am. v. Verizon Internet Services, Inc., 351 F.3d. 1229, 1233 (D.C. Cir. 2003).

¹³¹ RIAA v. THE PEOPLE: TWO YEARS LATER, *supra* note 97, at 5.

¹³² *Id.* at 2.

¹³³ *Id.*

¹³⁴ Complaint at 3-5, Atlantic Recording Corp. v. Huggins, No. 05 Civ. 1534 (E.D.N.Y. Mar. 24, 2005), available at http://codewarriorz.clawz.com/atlantic_huggins_complaint.pdf. See also 17 U.S.C.A. § 501 (West 2000) (providing that anyone who violates an exclusive right of a copyright holder may be liable for copyright infringement).

¹³⁵ See, e.g., Atlantic, No. 05 Civ. 1534 at 4.

rights in section 106 of the Copyright Act.¹³⁶ Proving ownership of the allegedly infringed copyrights is not difficult because most record companies file copyright registrations with the Copyright Office pursuant to section 408 of the Copyright Act,¹³⁷ prior to publication or shortly thereafter. However, it is more difficult to show that one of the exclusive rights was violated. Foster, a defendant in a copyright infringement action, stated in her answer that the claim was commenced without her having any actual knowledge or information that she participated in such illegal activities.¹³⁸ Subsequently, Foster demanded that the plaintiffs provide the dates of the alleged downloading and the files involved.¹³⁹ The plaintiffs, unable to meet the demand, filed a motion to dismiss the action with prejudice.¹⁴⁰ While the RIAA did not contest the demand in this case, it did challenge the demand for such specificity in *Goldshteyn*.¹⁴¹

Goldshteyn claimed that the plaintiffs failed to meet the specificity standards espoused under Rule 8(a) of the Federal Rules of Civil Procedure¹⁴² because the plaintiffs failed to allege the individual

¹³⁶ See *Napster*, 239 F.3d at 1013. See also 17 U.S.C.A. § 106.

¹³⁷ 17 U.S.C.A. § 408 (West 2000).

¹³⁸ See answer filed in *Capitol Records, Inc. v. Foster*. *Capitol Records, Inc. v. Foster*, Case No. 04-1569-W, at 9 (W.D. Okla. 2006), available at http://www.ilrweb.com/viewILRPDF.asp?filename=capitol_foster_amendanscounterclaims.

¹³⁹ Eric Bangeman, *RIAA Loses in File Sharing Case*, ARSTECHNICA.COM, <http://arstechnica.com/news.ars/post/20060713-7257.html>.

¹⁴⁰ Dismissal at 1, *Capitol Records, Inc. v. Foster*, No. Civ. 04-1569-W (W.D. Okla. July 13, 2006), available at http://www.ilrweb.com/viewILRPDF.asp?filename=capitol_foster_dismissal. See also Bangeman, *supra* note 139.

¹⁴¹ *Maverick Recording Co. v. Goldshteyn*, No. CV-05-4523 (DGT), 2006 WL 2166870 (E.D.N.Y. July 31, 2006).

¹⁴² FED. R. CIV. P. 8(a).

instances or exact times of infringement.¹⁴³ However, the court noted that plaintiffs need not provide the specific instances of infringement to withstand a motion to dismiss for failure to state a claim upon which relief can be granted.¹⁴⁴ From the brief opinion, an inference may be made that the court believed such specifics would be better dealt with through discovery.

Though the court upheld the sufficiency of the pleadings,¹⁴⁵ the ruling begs the question: How will the plaintiff prove specific instances of direct infringement if a trial ensued? Of course, during discovery a subpoena to the defendant's ISP will be issued and the specific instances of infringement may be discovered.¹⁴⁶ More than likely, however, the RIAA or the constituent record companies have hired outside help to scour the P2P networks. Alternatively, perhaps the RIAA or the record companies that make up the conglomerate will hire private investigators to search out infringing users' IP addresses and monitor their activity. It is this last activity that alleged copyright infringers have objected to in their answers to the complaint. Part II.B examines each counterclaim.

¹⁴³ See *Goldshteyn*, 2006 WL 2166870, at *2.

¹⁴⁴ See *id.* at *3 (citing *Capitol Records, Inc. v. Wings Digital Corp.*, 218 F. Supp. 2d 280, 284 (E.D.N.Y. 2002)).

¹⁴⁵ See *Goldshteyn*, 2006 WL 2166870, at *5.

¹⁴⁶ However, ISPs do not maintain such specific records of a user's activity. This fact is most evidenced by former Attorney General Alberto Gonzales' efforts to require ISPs to keep track of customers' online activity. See Declan McCullagh, *Gonzales: ISPs Must Keep Records on Users*, Sept. 20, 2006, CNETNEWS.COM, http://news.com.com/Gonzales+ISPs+must+keep+records+on+users/2100-1028_3-6117455.html (last modified Sept. 20, 2006). This issue will be addressed *infra* Part II.D.

B. Assertion of Privacy Rights Are Not a Viable Counterclaim for Active Copyright Infringers

The Fourth Amendment¹⁴⁷ only protects individuals from state or federal action.¹⁴⁸ Consequently, states are left to regulate privacy concerns within the home arising from invasions from private actors.¹⁴⁹ There have been three counterclaims that defendants in copyright infringement actions have routinely set forth in their answers to complaints filed by record companies. Those claims are common law trespass to chattels, common law invasion of privacy, and an invocation of the Computer Fraud and Abuse Act.¹⁵⁰

1. Common Law Trespass to Chattels

A private party may be liable for intentional trespass to chattels by either dispossessing another of the chattel, using the chattel, or interfering with the chattel that was in possession of another.¹⁵¹ Moreover, if the chattel's quality or value is impaired, or the possessor was deprived of use of the chattel for a substantial time, then the

¹⁴⁷ U.S. CONST. amend. IV, states, in pertinent part: "The right of the people to be secure in their persons, houses, papers . . . against unreasonable searches and seizures, shall not be violated"

¹⁴⁸ See, e.g., *Couch v. United States*, 409 U.S. 322, 336 (1973) (holding a Fourth Amendment claim cannot exist where there is no governmental action).

¹⁴⁹ For example, states have burglary, robbery, and trespass statutes at their disposal. There are also common law trespass and trespass to chattels remedies. However, defendants have the ability to invoke the Computer Fraud and Abuse Act. 18 U.S.C.A. § 1030 (West 2000).

¹⁵⁰ See Answer at 6-8, *Atlantic Recording Corp. v. Andersen*. *Atlantic Recording Corp. v. Andersen*, No. CV 05-933 AS, at 6-8 (D. Or. Sept. 30, 2005), available at http://info.riaalawsuits.us/atlantic_andersen/answer.cc.final.actual.pdf [hereinafter "Andersen Answer"]. Because there are various distinctions among the several States regarding application of these principles, the Restatement of Torts will serve as a proper guide.

¹⁵¹ See RESTATEMENT (SECOND) OF TORTS § 217 (2007).

trespasser may be liable.¹⁵² *Compuserve, Inc. v. Cyber Promotions, Inc.*¹⁵³ involved an action for electronic trespass to chattels. The plaintiff, Compuserve, filed the action against Cyber Promotions because the defendant sent bulk, unsolicited email advertisements to Compuserve's customers.¹⁵⁴ The court recognized that the Restatement Second of Torts defined "intermeddling" as intentional physical contact with a chattel.¹⁵⁵ Yet, the physical contact must produce some type of harm to the property, or a loss of value, to put forth a prima facie case; actual damage must be shown.¹⁵⁶ In issuing an injunction against Cyber Promotions, the court noted that Compuserve was unduly burdened by the bulk mailings because its computer systems were forced to store mass undeliverable emails, and such storing drained the processing power of Compuserve's computers.¹⁵⁷

As *Compuserve* illustrates, a claim of trespass to chattels must allege actual damage in order to present a prima facie case. Tanya Andersen's answer contained a counterclaim for trespass to chattels.¹⁵⁸ She alleged the record label employed a company called MediaSentry to "break into [her] personal computer . . . to secretly spy . . . and steal information or remove files."¹⁵⁹ However, the answer alleged no actual damage to the chattel—her computer.¹⁶⁰ Therefore, such a claim by a direct infringer of copyright must fail.

¹⁵² See *id.* at § 218.

¹⁵³ 962 F. Supp. 1015 (S.D. Ohio 1997).

¹⁵⁴ *Id.* at 1017.

¹⁵⁵ *Id.* at 1021 (citing RESTATEMENT (SECOND) OF TORTS § 217 cmt. e).

¹⁵⁶ *Id.* at 1022-23. See also RESTATEMENT (SECOND) OF TORTS § 217.

¹⁵⁷ *Compuserve*, 962 F. Supp. at 1022.

¹⁵⁸ Andersen Answer, *supra* note 150, at 6.

¹⁵⁹ *Id.*

¹⁶⁰ *Id.* at 6-7.

Furthermore, much like a possessor of a chattel has a right to use reasonable force to protect the chattel,¹⁶¹ a copyright holder should have the right to use reasonable force to protect the profitability and exclusive rights of its musical copyright by invading a copyright infringer's home computer. The Restatement Second of Torts supports this proposition.¹⁶² Section 260, subsection two of the Restatement states that one may commit an act which could be deemed trespass to chattels, but would not incur liability so long as the actor reasonably believes that the action is necessary to protect his chattels.¹⁶³

Therefore, trespass to chattels is a question of which party has the greater right—the party asserting trespass to her personal computer, or the party asserting an infringement of copyright and engaging in trespass to chattel to protect the viability of its copyright? The answer should depend on whether a copyright can be treated as a chattel.¹⁶⁴ Yet, without a claim of actual damage to her personal computer, Tanya Andersen, or any other defendant claiming trespass to chattels, would not have a *prima facie* case.¹⁶⁵

2. *Common Law Invasion of Privacy*

A private party who intentionally intrudes upon the seclusion of another's private affairs in a manner that is highly offensive to a

¹⁶¹ RESTATEMENT (SECOND) OF TORTS § 218 cmt. e.

¹⁶² *Id.* at § 260(1).

¹⁶³ *Id.* To sufficiently express the point that copyrighted materials are chattels, we must assume copyrights are much like tangible property. *See infra* Part II.C.

¹⁶⁴ *See infra* Part II.C.

¹⁶⁵ However, should the defense claim actual damages, its viability depends on whether a copyright can be construed as physical property. *See infra* Part II.C.

reasonable person may incur liability for invasion of privacy.¹⁶⁶ Under Rule 8(a) of the Federal Rules of Civil Procedure, a pleading requires a short and plain statement of the claim.¹⁶⁷ The Andersen Answer would seem to meet the pleading requirements.¹⁶⁸ However, the Restatement explains under comment d to section 652B that the interference must be substantial and highly offensive to a reasonable person. The comment begs the question: would an invasion by a private party to investigate the infringement of its copyright be highly offensive to a reasonable person who has infringed such copyright? Surely, any law abiding citizen would answer in the negative.

For example, in *Munley v. ISC Financial House, Inc.*,¹⁶⁹ the plaintiff instituted an invasion of privacy action against the defendant ISC Financial House for harassing phone calls to the plaintiff, plaintiff's apartment manager, and plaintiff's former employer, and for inquiries to the plaintiff's neighbors about the type of furniture located within the plaintiff's home.¹⁷⁰ The defendant made phone calls and inquiries because the plaintiff defaulted on payments to ISC Financial House.¹⁷¹ The court noted that a creditor has a right to take reasonable action to pursue a debtor, although it may result in an invasion of privacy.¹⁷² In concluding that the invasion of privacy claim must fail because the conduct exhibited by the defendant was not highly offensive to a reasonable person, the court noted the defendant had a le-

¹⁶⁶ RESTATEMENT (SECOND) OF TORTS § 652B (1977).

¹⁶⁷ FED. R. CIV. P. 8(a).

¹⁶⁸ See Andersen Answer, *supra* note 150, at 8.

¹⁶⁹ 584 P.2d 1336 (Okla. 1978).

¹⁷⁰ *Id.* at 1337-38.

¹⁷¹ *Id.* at 1337.

¹⁷² *Id.* at 1339-40.

gitimate debt, and the plaintiff was merely trying to interfere with the defendant's collection of the debt.¹⁷³ Thus, under *Munley*, an invasion of privacy claim will fail if a plaintiff committed a wrong against the defendant because the defendant's conduct would not be highly offensive to a reasonable person. The defendant would merely be attempting to correct that wrong.

The rule is analogous to section 9-609 of the Uniform Commercial Code ("UCC").¹⁷⁴ Under section 9-609 a creditor may repossess collateral in the possession of a debtor without constituting a breach of privacy, so long as a breach of the peace does not occur.¹⁷⁵ In *Thompson v. First State Bank of Fertile*,¹⁷⁶ the court held that it was reasonably necessary for the "repo-man" to enter Thompson's property to take possession of the automobile because Thompson had defaulted on his loan.¹⁷⁷ The court applied Minnesota's version of section 9-609 of the U.C.C.¹⁷⁸

Recognizing that section 9-609 of the U.C.C. applies solely to secured transactions, it can be said that both creditors and copyright holders are protecting their economic interests. Therefore, much like a creditor, a copyright holder who has been victimized by the unauthorized uploading and downloading of its copyrights by a direct in-

¹⁷³ *Id.* at 1340.

¹⁷⁴ U.C.C. § 9-609 (2000) states, in pertinent part: "After default, a secured party . . . may take possession of the collateral . . . without judicial process, if it proceeds without breach of the peace." From a cursory inspection of cases involving section 9-609, it appears the section has not been applied to cases outside the realm of secured transactions. Such novel uses of existing law however, should not prevent another wholly separate body of law from adopting its principles. *See, e.g., Grokster*, 545 U.S. 913; *Sony*, 464 U.S. 417.

¹⁷⁵ U.C.C. § 9-609(a)-(b).

¹⁷⁶ 709 N.W.2d 307 (Minn. 2006).

¹⁷⁷ *Id.* at 313.

¹⁷⁸ *See id.* at 310-11. *See also* MINN. STAT. ANN. § 336.9-609 (West 2006).

fringer may attempt to correct that wrong by gathering evidence against the direct infringer to commence a lawsuit. Should a direct infringer, like Andersen, claim an invasion of privacy, the claim would fail because the record company's conduct of investigating a home computer would not be highly offensive to a reasonable person, since the direct infringer was in possession of the record label's personal property, or rather, in possession of its economic interests.¹⁷⁹

3. *The Computer Fraud and Abuse Act*

The Computer Fraud and Abuse Act ("CFAA")¹⁸⁰ guards against the unauthorized intrusion into a protected computer with the intention to steal government secrets, defraud individuals, and knowingly transmit malicious coding software which causes damage.¹⁸¹ The CFAA defines "protected computer" as any computer used in interstate communication.¹⁸² Consequently, a home computer is a "protected computer" within the meaning of the CFAA. The CFAA appears to be the federal corollary to the common law action of trespass to chattels.¹⁸³ Both the Restatement and the CFAA require a showing of damage to the chattel—the computer.¹⁸⁴ Therefore, an analysis of a claim under the CFAA would be akin to a claim for trespass to chattels.

¹⁷⁹ See *Munley* for the analogous argument. 584 P.2d at 1340. "[ISC Financial House] had a legitimate debt owed to it by [Munley] and her former husband and [Munley] was in possession of personal property securing the debt." *Id.* Again, this analogy depends on whether a copyright can be construed as tangible property. See *infra* Part II.C.

¹⁸⁰ 18 U.S.C.A. § 1030.

¹⁸¹ See *id.* § 1030(a)(1)-(5).

¹⁸² *Id.* at § 1030(e)(2)(B).

¹⁸³ Compare 18 U.S.C.A. § 1030, with RESTATEMENT (SECOND) OF TORTS § 217.

¹⁸⁴ See 18 U.S.C.A. § 1030(a)(5); RESTATEMENT (SECOND) OF TORTS § 217.

However, the CFAA also contains a provision prohibiting intentional unauthorized access to obtain information.¹⁸⁵ The mounting of a defense against a violation of the CFAA hinges on the definition of “information.” Yet, the CFAA failed to define “information.”¹⁸⁶ Furthermore, the legislative record is devoid of any indication as to the definition of “information.”¹⁸⁷ Perhaps the drafters thought “information” was to be construed according to its usual definition: “The act of informing or the condition of being informed; communication of knowledge.”¹⁸⁸

The Andersen Answer included a counterclaim for a violation of the CFAA in that private information of the music files contained within Andersen’s home computer was gathered.¹⁸⁹ Construing information according to the usual definition raises the question of whether the CFAA intended “information” to mean proprietary information. If so, it would be difficult for Andersen to win on her CFAA claim.¹⁹⁰ The copyrighted music contained on Andersen’s computer is the copyright holder’s property, unless Andersen herself purchased the music.¹⁹¹ As the rightful proprietary owners of the copyrighted music, the record companies would have a right to enter another’s property by virtue of the common law defense to trespass to

¹⁸⁵ 18 U.S.C.A. § 1030(a)(2)(C).

¹⁸⁶ *See id.* at § 1030(e).

¹⁸⁷ *See generally* H.R. CONF. REP. No. 98-1159 (1984) (Conf. Rep.), as reprinted in 1984 U.S.C.C.A.N. 3710 (1984).

¹⁸⁸ THE AMERICAN HERITAGE DICTIONARY 660 (2d College ed. 1985).

¹⁸⁹ Andersen Answer, *supra* note 150, at 7.

¹⁹⁰ Section 1030 reveals that the various provisions deal with proprietary information. For example, the provisions deal with bank account fraud, or the use of proprietary information to extort. *See* 18 U.S.C.A. § 1030.

¹⁹¹ The Andersen Answer fails to claim that the music contained within her home was purchased. *See* Andersen Answer, *supra* note 150, at 7.

chattels.¹⁹² Consequently, the CFAA claim must fail if the information gathered by MediaSentry's inspection of Andersen's home computer was not Andersen's property in the first place.¹⁹³

A record company would withstand an allegation of the above three claims if a copyright can be construed as tangible property. The following section addresses that point.

C. Musical Recording Copyrights are Much Like Tangible Property

The preceding Section discussed how a record company may defeat counterclaims of trespass to chattels, invasion of privacy, and a violation of the CFAA. However, the record companies' defense depends largely on construction of a copyright as tangible property. For a record company to assert a right to invade a direct infringer's home computer, it must allege that its sound recording copyrights have been infringed by direct infringers.

A copyright holder of a sound recording enjoys all the exclusive rights enumerated in 17 U.S.C.A. section 106, except where limited under section 114(a)-(b).¹⁹⁴ Section 101 of the Copyright Act de-

¹⁹² See Part II.B.1 for a general discussion of the common law defense to trespass to chattels which gives the right to enter another's property to regain control of illegally obtained property.

¹⁹³ An exhaustive review of cases having dealt with any claim arising under the CFAA claim revealed that no court has dealt with whether "information" means proprietary information. This review involved searching "section 1030" on LexisNexis and Westlaw and examining every case that the search revealed.

¹⁹⁴ Compare 17 U.S.C.A. § 106 with 17 U.S.C.A. § 114(a)-(b) (West 2000). Section 114(a) states: "The exclusive rights of the owner of copyright in a sound recording are limited to the rights specified by clauses (1), (2), (3) and (6) of section 106, and do not include any right of performance under section 106(4)." Section 114(b) states, in pertinent part:

The exclusive right of the owner of copyright in a sound recording under clause (1) of section 106 is limited to the right to duplicate the sound recording in the form of phonorecords or copies that directly or

defines sound recordings as “works that result from the fixation of a series of musical, spoken, or other sounds”¹⁹⁵ A sound recording is different from a phonorecord because a phonorecord is the material object that contains the music, such as a CD.¹⁹⁶ A record company claiming infringement of copyright could not claim that its phonorecord copyright has been infringed because direct infringers utilizing P2P software have reduced the phonorecord to an MP3 file. The file itself contains the actual sounds that make up a song.

Because the MP3 file contains the musical sounds that make up a work, an MP3 file can be treated as tangible property. While this is not the precise holding of *Bridgeport Music, Inc. v. Dimension Films*,¹⁹⁷ the case did conclude that sound recordings were like physi-

indirectly recapture the actual sounds fixed in the recording. The exclusive right of the owner of copyright in a sound recording under clause (2) of section 106 is limited to the right to prepare a derivative work in which the actual sounds fixed in the sound recording are rearranged, remixed, or otherwise altered in sequence or quality. The exclusive rights of the owner of copyright in a sound recording under clauses (1) and (2) of section 106 do not extend to the making or duplication of another sound recording that consists entirely of an independent fixation of other sounds, even though such sounds imitate or simulate those in the copyrighted sound recording.

17 U.S.C.A. § 114(b).

¹⁹⁵ 17 U.S.C.A. § 101 (West 2000) states in pertinent part:

“Sound recordings” are works that result from the fixation of a series of musical, spoken, or other sounds, but not including the sounds accompanying a motion picture or other audiovisual work, regardless of the nature of the material objects, such as disks, tapes, or other phonorecords, in which they are embodied.

¹⁹⁶ 17 U.S.C.A. § 101 states in pertinent part:

“Phonorecords” are material objects in which sounds, other than those accompanying a motion picture or other audiovisual work, are fixed by any method now known or later developed, and from which the sounds can be perceived, reproduced, or otherwise communicated, either directly or with the aid of a machine or device. The term ‘phonorecords’ includes the material object in which the sounds are first fixed.

¹⁹⁷ 410 F.3d 792 (6th Cir. 2005).

cal property.¹⁹⁸

Bridgeport Music involved the digital sampling of a two-second piece of the plaintiff's song.¹⁹⁹ The specific piece taken was part of a guitar solo in the original work.²⁰⁰ The defendant did not deny copying the altered version of the two-second piece and inserting it into his own work.²⁰¹ The appellate court reversed and distinguished the analysis for an infringement of a musical composition copyright from that of sound recording infringement. Therefore the district court erred in applying a *de minimis* inquiry.²⁰²

In rejecting the *de minimis* or substantial similarity test, the court noted section 114(b) of the Copyright Act gave "sound recording copyright holders the exclusive right 'to duplicate the sound recording in the form of phonorecords'"²⁰³ This meant that persons may imitate the sound recording, but, by no means may someone copy the sound recording itself.²⁰⁴ When a direct infringer downloads or uploads a song to or from a P2P network, the direct infringer is essentially copying the sound recording itself. The CD or its packaging are not copied, but the sound recording embodied within the CD is copied. "For the sound recording copyright holder, it is not the 'song' [itself,] but the sounds that are fixed in the medium of his choice. When those sounds are . . . taken directly from

¹⁹⁸ See *id.* at 802 (holding sounds sampled directly from a fixed medium constitute a physical taking, as opposed to an intellectual taking).

¹⁹⁹ *Id.* at 796.

²⁰⁰ *Id.*

²⁰¹ *Id.*

²⁰² *Bridgeport Music*, 410 F.3d at 798.

²⁰³ *Id.* at 800.

²⁰⁴ *Id.*

that fixed medium. . . . [i]t is a physical taking rather than an intellectual one.”²⁰⁵ Consequently, the court adopted a strict sound recording copyright rule that even if a two-second sample was taken from a song, it is a physical taking of something with value, and any violator would be held liable for infringement.²⁰⁶

The *Bridgeport Music* court was correct in its characterization that copying a sound recording copyright is a “physical taking” because sound recordings can only be removed directly from the physical medium in which they are embodied, such as a CD. Such takings are physical in the sense that the phonorecord is a tangible object. Once a sound recording is removed from its tangible medium, every subsequent transmission can be described as having its origin in a physical taking. It follows that downloaders and uploaders of digital music are transmitting digital files that have their origin in a tangible medium, with every succeeding transmission being a vicarious physical taking. Thus, each taking of a digital sound recording may be analogized with the first physical-taking of a tangible medium.

Consequently, because sound recording copyrights may be considered tangible property, viable defenses for record companies against claims of trespass to chattels, invasion of privacy, and violations of the CFAA become readily apparent.²⁰⁷ Construing a musical

²⁰⁵ *Id.* at 802.

²⁰⁶ *Id.* at 801-02.

²⁰⁷ *But see Dowling v. United States*, 473 U.S. 207 (1985). The *Dowling* case dealt with the application of the National Stolen Property Act to bootleg phonorecords. *Id.* at 208. The Supreme Court had to determine whether the bootleg phonorecords were stolen, converted, or taken by fraud within the meaning of the statute, “only in the sense that they were manufactured and distributed without the consent of the copyright owners of the musical compositions performed on the records.” *Id.* at 208, 215-16. The Court also had to determine whether the bootleg phonorecords were “goods” or “wares” within the meaning the statute.

copyright as tangible property, capable of being possessed, it follows that a copyright would therefore be capable of being physically protected as well.²⁰⁸

D. Further Showings of a Derogation of Privacy Rights

As discussed earlier, the effect of mass unauthorized downloading of copyrighted music has led to lawsuits against direct infringers. The direct infringers, in turn, filed invasion of privacy type claims. However, the government is not siding with the infringers.

In 2002, Howard Berman, a representative of California in the House of Representatives, introduced the Privacy Prevention Bill (“The Bill”) to allow a copyright holder to electronically enter a direct infringer’s computer.²⁰⁹ The Bill essentially stated that a copyright holder would not be liable as a matter of law for interfering with the rights of direct infringers, so long as no damage was done to any data contained on the infringer’s computer.²¹⁰ The Bill was not en-

Id. at 216. The Court, in rejecting the application of the statute to copyrights, stated that copyrights were not ordinary chattels because an infringer cannot assume physical control over a copyright, nor deprive its owner of its use. *Id.* at 216-17. Therefore, the Court noted that copyrights cannot be possessed like ordinary goods. *Id.* at 217. Yet, this holding is outdated. The case took place in 1985, before *Napster* and the mass infringement of copyright that followed. Most notably, however, the case dealt with a musical composition copyright, not a sound recording copyright. *Id.* at 212. Consequently, the *Bridgeport Music* holding is not limited by *Dowling*.

²⁰⁸ See *supra* Part II.B.1-3 to understand how construing a musical copyright as physical copyright would help defeat claims enumerated therein.

²⁰⁹ Declan McCullagh, *Could Hollywood Hack your PC?*, CNETNEWS.COM, http://news.com.com/Could+Hollywood+hack+your+PC/2100-1023_3-945923.html (last modified July 24, 2002). See also H.R. 5211, 107th Cong. § 514(a) (2002) [hereinafter *The Bill*].

²¹⁰ *The Bill* states, in pertinent part:

Notwithstanding any State or Federal statute or other law . . . a copyright

acted due to its late introduction in the 2002 term.²¹¹ However, with the conclusion of the November 2006 election, the Democrats have taken control of Congress and The Bill may yet become a reality.²¹²

In September 2006, then Attorney General Alberto Gonzales called for ISPs to retain a record of their customers' online activities.²¹³ Gonzales lobbied for support under the guise of preventing crime against child pornography.²¹⁴ The Bill was officially introduced in the House of Representatives on February 6, 2007.²¹⁵ However, the Bill is quite broad as it only mentions that the records would be retained under regulations issued by the Attorney General.²¹⁶ No vote has taken place on the Bill.²¹⁷

In October 2006, FBI Director Robert Mueller called on ISPs

owner shall not be liable in any criminal or civil action for disabling, interfering with, blocking, diverting, or otherwise impairing the unauthorized distribution, display, performance, or reproduction of his or her copyrighted work on a publicly accessible peer-to-peer file trading network, if such impairment does not, without authorization, alter, delete, or otherwise impair the integrity of any computer file or data residing on the computer of a file trader.

H.R. 5211, *supra* note 209.

²¹¹ See Kristine Pesta, Comment, *The Piracy Prevention Bill, H.R. 5211: The Second Generation's Answer to Copyright Infringement over Peer-To-Peer Networks*, 33 SW. U. L. REV. 397, 417 (2004) (citing *Congressman May Back Off on Tactics in Anti Piracy Bill*, HOUSTON CHRON., Sept. 27, 2002, at 10).

²¹² See Declan McCullagh, *What the Democrats' Win Means for Tech*, CNETNEWS.COM, http://news.com.com/What+the+Democrats+win+means+for+tech/2100-1028_3-6133833.html (last modified Jan. 2, 2007). McCullagh wrote that if Representative Howard Berman becomes the chairman of copyright subcommittee, the recording industry would have an ally. Representative Berman did indeed become the chairman of the copyright subcommittee, however, there has not been any further legislative activity regarding The Bill. See U.S. House of Representatives Committee on the Judiciary, <http://judiciary.house.gov/committeestructure.aspx?committee=3> (last visited Feb. 1, 2008).

²¹³ See McCullagh, *supra* note 146.

²¹⁴ *Id.*

²¹⁵ See H.R. 837, 110th Cong. § 6 (as introduced by Representative Smith, Feb. 6, 2007).

²¹⁶ *Id.*

²¹⁷ In an exhaustive search of the legislative history of the House of Representatives, it appears that no further action has taken place on House Bill 837.

to retain customer records to help with the war on terrorism.²¹⁸ In presenting the need for such legislation, Mueller stated that before some offenders could be caught, ISPs had deleted the information that would have helped build a case against such criminals.²¹⁹

In May 2007, then Attorney General Gonzales proposed the Intellectual Property Protection Act of 2007 ("IPPA").²²⁰ The IPPA would criminalize attempted copyright infringement.²²¹ More importantly however, the IPPA would allow more wiretaps for infringement, and attempted infringement investigations.²²² The proposal, among others, is currently being reviewed by Representative Berman's office.²²³

The foregoing shows that a further derogation of privacy rights is occurring, and legislation may be passed in the immediate future. Should such legislation be enacted, the Internet would be saturated with law enforcement and private investigation firms seeking out copyright infringers and criminal offenders. If Representative Berman's bill were eventually enacted, a record company would no longer need to employ private investigation firms. A record company

²¹⁸ Declan McCullagh, *FBI Director Wants ISPs to Track Users*, CNETNEWS.COM, http://news.com.com/FBI+director+wants+ISPs+to+track+users/2100-7348_3-6126877.html (last modified Oct. 18, 2006).

²¹⁹ *Id.*

²²⁰ Declan McCullagh, *Gonzales Proposes New Crime: 'Attempted' Copyright Infringement*, CNETNEWS.COM (May 15, 2007), http://news.com.com/8301-10784_3-9719339-7.html.

²²¹ See Letter from Richard A. Hertling, Principal Deputy Assistant Attorney General, to Nancy Pelosi, Speaker, U.S. House of Representatives 10 (May 14, 2007), available at <http://politechbot.com/docs/doj.intellectual.property.protection.act.2007.051407.pdf>. Attached to the letter is the proposed Intellectual Property Protection Act of 2007. *Id.* at 1. See also McCullagh, *supra* note 220.

²²² McCullagh, *supra* note 220.

²²³ *Id.*

employee could log on to any popular P2P network and disable infringing users from the comfort of the record company's office.²²⁴ Even if Berman's bill is not enacted, Gonzales' recommendation may be successful and a record company could go directly to an ISP for a record of any customers' online activity.

Enacting such bills would help protect the viability of musical copyrights and secure royalty payments to those artists whose record labels have already recouped on their investment, while curbing the downward spiral of the music industry.²²⁵ Of course, consumers may prevent the situation without the enactment of debilitating statutes gaining access to consumers' personal life by comporting: purchasing physical albums or the digital counterpart off such digital stores such as the iTunes Music Store.²²⁶

In concluding the preceding Section, a quote from Cary Sherman, President of the RIAA seems apt.

[O]ur right to privacy does not include a right to commit illegal acts anonymously. You or I may have a right to keep our banking transactions private, but when we stick a gun in a teller's face and ask for the contents of the cash drawer, the bank is more than entitled to take our picture with a security camera. The same is true on the Internet. Offering to upload music files without permission so millions of strangers can

²²⁴ While the final language to such a bill is yet to be determined, the Fourth Amendment may stand as a barrier because the federal government would be placing its "power, property and prestige behind" a record company's actions. See *Burton v. Wilmington Parking Auth.*, 365 U.S. 715, 725 (1961).

²²⁵ Ethan Smith, *Sales of Music, Long in Decline, Plunge Sharply*, WALL ST. J., Mar. 21, 2007, at A1 (reporting the music industry has been in a seven-year decline, and that in the first three months of 2007, sales of CDs had plummeted twenty percent from the previous year).

²²⁶ However, the digital music sales have not helped to offset the decline in music sales across the board. See *id.*

copy them off the Internet is neither a private act nor a legal one. Should those who engage in this gratuitous giveaway of other people's property be able to conceal their identity behind computer numbers or made-up screen names?²²⁷

III. CONCLUSION

Copyrights vest authors with a monopoly over the created work. This monopoly, constitutional in origin, includes the rights to distribute and reproduce the works. When a direct infringer downloads or uploads an author's musical work for mass consumption by the P2P public, that person infringes upon the author's rights. Holders of a copyright in a musical work must be allowed to protect the profitability or viability of their copyrights, even if that means invading the home computer of suspected direct infringers. Moreover, the failure of certain digital copyright protection schemes demonstrate the urgency with which courts and the federal government should take action.²²⁸

Characterizing a home computer invasion as a violation of direct infringers' privacy rights would contravene the purpose of the Copyright Act—to give a monopoly to authors for a limited time. Allowing privacy type claims against copyright holders would prevent the expeditious remedy of unauthorized trafficking of copyrighted works.

At Napster's peak, 260 million albums were being

²²⁷ See Pesta, *supra* note 211, at 414 (quoting Cary Sherman, *Issue is Piracy, Not Privacy*, USA TODAY, Jan. 23, 2003, at A11).

²²⁸ See generally Pesta, *supra* note 211 (discussing the various forms of failed digital copyright protection schemes).

downloaded every month.²²⁹ If the average price of each physical album was ten dollars, the music industry would be deprived of 2.6 billion dollars. That income could be used to clear some artists of the debt owed to their respective record companies, and allow the individual artists to begin receiving royalty payments.

Because many record labels are reportedly experiencing a financial decline,²³⁰ judges presiding over direct infringement of musical copyright cases should not hold copyright holders—the record labels—liable for trespass to chattels, invasion of privacy, or violating the CFAA. Courts should recognize that the rights of both individuals and copyright holders are constitutional in origin. Yet, persons derive their privacy rights from the Constitution only when government action is involved. When a direct infringer downloads music from the Internet, they are violating the Constitutional rights of a copyright holder. To say that one can illegally download music through a veil of secrecy is tantamount to saying a jailed convict should have the right to vote while in prison because his right to vote is derived from the Constitution.

However, direct infringers do not enjoy privacy protection when engaged in illegal downloading. Private firms, which are not involved with government action, are investigating home computers. Therefore, a copyright holder, deriving the right to protect its property from the Constitution, has a paramount right to that of a direct infringer attempting to protect his computer from an invasion.

Alternatively, should courts find the foregoing arguments un-

²²⁹ See Bainwol, *supra* note 3.

²³⁰ Smith, *supra* note 225.

persuasive, the possibility of government action is looming. As demonstrated in Part II.D., government action would break down the remaining walls of privacy should courts not protect the paramount rights of copyright owners.

The search for an answer to the mass infringement of copyright received an even greater push in May 2007 when the record company EMI debuted the availability of digital music without copy restrictions on Amazon.com and the iTunes Music Store.²³¹ Unrestricted digital music, free of digital rights management software ('DRM'), or DRM-free music, as it is called in the tech-world, will allow interoperability between various MP3 music players.²³² However, the motive for the shift to DRM-free music can best be questioned as whether the downward slide in music sales has led record companies to shift their marketing strategies. Will DRM-free music allow for a greater market share amongst all consumers owning MP3 players?

Record companies are keeping a close eye on the EMI venture because an increase in market share could mean the revitalization of the music industry and spur the greater availability of DRM-free music from other major record companies.²³³ Yet, EMI's failure could

²³¹ Greg Sandoval, *Apple, Amazon May Hold Future of DRM-free Music*, CNETNEWS.COM, http://news.com.com/Apple%2C+Amazon+may+hold+future+of+DRM-free+music/2100-1027_3-6184509.html?tag=nefd.top. See also Candace Lombardi, *iTunes Goes DRM-free with EMI*, CNETNEWS.COM, http://news.com.com/iTunes+goes+DRM-free+with+EMI/2100-1027_3-6187457.html (last modified May 31, 2007); Caroline McCarthy, *EMI, Apple Partner on DRM-free Premium Music*, CNETNEWS.COM, http://news.com.com/EMI,+Apple+partner+on+DRM-free+premium+music/2100-1027_3-6172398.html (last modified Apr. 3, 2007).

²³² See Lombardi, *supra* note 231; Sandoval, *supra* note 231; McCarthy, *supra* note 231.

²³³ Sandoval, *supra* note 231.

also mean greater copy restrictions on digital music.²³⁴ Yet, what does the EMI venture mean for the privacy rights of those users purchasing DRM-free music and making them available on P2P sites?

The repudiation of copy-protection on digital music could mean that DRM-free music will be policed on the Internet more than ever before, in the absence of formal legislation. A recent technological breakthrough, Clouseau, boasts it can stop all P2P piracy without any alleged violation of privacy rights.²³⁵ Clouseau was recently used in “Operation D-Elite,” a federal crackdown on P2P file sharing.²³⁶

However, technology moves forward, and so too must legislation. It is vital to protect the rights of artists and composers guaranteed by the Constitution of the United States in a rapidly advancing digital world, at the expense of the privacy rights of those infringing copyright.

²³⁴ *Id.*

²³⁵ See generally Press Release, Billboard Publicity Wire, Clouseau® Cracks the Code to Destroy P2P Piracy (Apr. 19, 2007), available at <http://billboard.prweb.com/releases/2007/4/prweb520200.htm>.

²³⁶ *Id.*