

SONY-BMG AND DIGITAL RIGHTS MANAGEMENT: THE OVEREXTENSION OF COPYRIGHT PROTECTION IN AUDIO RECORDINGS

I. INTRODUCTION

In response to widespread music piracy and the extensive unauthorized copying of compact discs (CDs) using personal computers (PCs), record companies have increasingly turned to Digital Rights Management (DRM) to protect their copyright rights in audio recordings. From 2003 to 2005, Sony-BMG (Sony) released fifty-two albums¹ that included different versions of DRM protection, MediaMax² and Extended Copyright Protection (XCP),³ which had the potential to severely corrupt the customer's PC to which they were copied. These DRM technologies were effective in the way they prevented customers from making mass copies of Sony CDs.⁴ However, the effectiveness of these protections was the result of extreme anti-circumvention measures that essentially deprived the customer of the use of his or her computer for music listening.⁵ Moreover, in many cases, the installation of this software on users' PCs was the result of remarkably misleading and suspicious conduct by Sony, and was often done

¹ This number represents approximately twenty-five million CDs. Artists releasing the albums include: Billie Holiday, Celion Dion, Earl Scruggs, My Morning Jacket, Neil Diamond, Pete Seeger, Trey Anastasio, and many more.

² Two versions of MediaMax were created, versions 3.0 and 5.0, by a company called SunnComm.

³ XCP was created by a British software company called First 4 Internet.

⁴ When operating correctly, the DRM would allow only three copies of a given CD to be made, and once uploaded onto a computer, the music could only be accessed with the special media player that accompanied the software and could only be downloaded onto some portable mp3 players.

⁵ See *infra* pp. 4-9.

without notice to consumers.⁶ In response to the undisclosed inclusion of these harmful DRM technologies on its CDs, many lawsuits were filed against Sony for violation of state, federal, and common laws. Since the initiation of these various lawsuits, however, most have been settled out of court between Sony and the affected parties.

Part II of this Note explores the use of DRM protection in general, and considers the legality of the steps taken by Sony to prevent the unauthorized copying of its recordings by consumers who lawfully purchased those recordings. Part III of this Note analyzes the applicable federal and state laws in light of Sony's actions, and reviews the potential liabilities incurred by Sony, who released CDs with potentially harmful or damaging software embedded within, the customers copying the CDs, and the people attempting to circumvent or remove the DRM software. In Part IV, this Note examines the legislative efforts that emerged as a result of Sony's conduct, and questions the propriety of the scope of protection that the Copyright Act currently affords owners of copyrighted audio recordings. Finally, this Note concludes that the state of copyright law regarding audio recordings is vulnerable in many ways, and needs to be amended to adapt to current trends in the online music market, technology, society, and in light of the public perception of abusive recording companies in the aftermath of Sony's digital rights *mismanagement*.

II. DIGITAL RIGHTS MANAGEMENT AND COPYRIGHT PROTECTION

⁶ See *infra* part II.

DRM refers to “[a]ny technology used to limit the use of software, music, movies or other digital data . . . [which] generally relies on some interaction between the media and the system that plays it.”⁷ Often, DRM technologies attempt to control or prevent access to or copying of digital media, which can otherwise be copied with very little cost or effort. Considering the ease with which CDs can be copied using PCs, many recording companies have naturally turned to DRM protection that is designed to limit or prevent the copying of CDs with computers.⁸ Sony’s DRM tactics were intended to prevent such copying, but, as we will see, they did so at the customer’s expense. Researchers at Princeton University’s Center for Information and Technology Policy conducted an in-depth analysis of Sony’s DRM technologies to evaluate their theoretical and realistic effects upon customer’s personal computers.⁹

A. *MediaMax*

⁷ Dictionary.com, Digital Rights Management, <http://dictionary.reference.com/browse/digital%20rights%20management>.

⁸ For an analysis of modern DRM technologies, see JOHN A. HALDERMAN, EVALUATING NEW COPY-PREVENTION TECHNIQUES FOR AUDIO CDS (July 2002), *available at* <http://www.cs.princeton.edu/~jhalderm/papers/drm2002.pdf>. Recent attempts to limit such copying include: corrupting the table of content on discs to confuse the computer and prevent it from reading the audio tracks on the CD; freezing the music that is uploaded onto the computer and requiring the user to go online and register and download an encrypted version of the lawfully purchased CD which has copy-prevention software embedded within; corrupting the audio tracks by inserting gaps or blocks into the songs which are read by a computer as actual music and burned onto a CD, which, when played, damages speakers with hisses and pops.

⁹ J. ALEX HALDERMAN & EDWARD W. FELTEN, CENTER FOR INFORMATION TECHNOLOGY POLICY, PRINCETON UNIVERSITY, LESSONS FROM THE SONY CD DRM EPISODE (Extended Version, Feb. 14, 2006), *available at* <http://itpolicy.princeton.edu/pub/sonydrm-ext.pdf>.

The first DRM protection introduced by Sony was MediaMax, which was released on thirty-seven albums, over twenty million CDs.¹⁰ MediaMax was primarily designed to prevent the unauthorized copying of Sony CDs. This was accomplished by automatically installing the DRM on the hard drive when the MediaMax CD was inserted into the computer. Indeed, when the CD was inserted into the drive and the end user license agreement (EULA) was presented on the screen, it would appear only one time for the user to accept or reject its terms. However, just before the EULA appeared,¹¹ MediaMax began activation of the protection software. In fact, “even before displaying a [EULA], MediaMax cop[ied] almost twelve megabytes of files and data related to the MediaMax player to the hard disk”¹² Thus, the software was installed and activated without obtaining the user’s consent.¹³ Moreover, the software would automatically install itself even when the user rejected the terms of the EULA, and, in some cases, remained permanently active.¹⁴

¹⁰ *Id.* at 4.

¹¹ MediaMax is automatically loaded on computers with Windows operating systems by way of the autorun feature provided by Windows. This option is not available on other operating systems, such as Linux and MacOS X, so the automatic loading element of MediaMax is only applicable to Windows computers. *Id.* at 5-6.

¹² *Id.* at 17.

¹³ *Id.* at 7.

¹⁴ Megan M. LaBelle, *The Rootkit Debacle: The Latest Chapter in the Story of the Recording Industry and the War on Music Piracy*, 84 DENV. U.L. REV. 79, 91 (2006). The MediaMax DRM remains permanently active when:

[T]he user inserts a MediaMax 3.0 CD and then later inserts a MediaMax 5.0 CD (or vice versa), the software will be active despite the user’s prior decision to decline the EULA. Similarly, inserting a 5.0 CD, rebooting your computer, and then inserting the same album or another CD with the 5.0 software will lead to the same result.

Id.

In addition to the ethical concerns posed by these tactics, MediaMax was deceptive in other ways as well. For example, the MediaMax EULA stated that “[t]he software will not be used at any time to collect any personal information from you, whether stored on your computer or otherwise.”¹⁵ However, despite this clause in the agreement, MediaMax did in fact obtain and transmit users’ personal information stored on their computers back to Sony and the manufacturer of the DRM, SunnComm.¹⁶ The program, which included its own media player, would contact the web server after a disc was inserted into the computer in order to display the album art or banner ads. Once contact was made, however, the player was connected to the web server, and “[t]hese connections allow[ed] the servers to log the user’s IP address, the date and time, and the identify of the album.”¹⁷ These features render MediaMax more akin to spyware rather than a DRM measure intended to secure copyright rights.

B. Extended Copyright Protection (XCP)

The second type of DRM introduced by Sony was XCP, which was released on fifty-two albums, representing more than four and a half million CDs.¹⁸ XCP featured many of the same functions as MediaMax, including automatic loading of the program after inserting the disc into the drive,¹⁹ incorporating its own restrictive media player,²⁰

¹⁵ MediaMax, End User License Agreement.

¹⁶ HALDERMAN & FELTEN, *supra* note 9, at 14.

¹⁷ *Id.* In addition to this information, MediaMax would also report the type of operating system and the version of Internet Explorer installed on the user’s computer. LaBelle, *supra* note 14, at 90-91.

¹⁸ HALDERMAN & FELTEN, *supra* note 9, at 4.

¹⁹ *Id.* at 5. “The first time an XCP-protected disc is inserted into a Windows machine, the Windows autorun feature launches the XCP installer.” *Id.* at 6.

²⁰ *Id.* “XCP and MediaMax provide their own proprietary media players... on each protected CD, that allow certain limited uses of the music subject to restrictions imposed by the copyright holder.” *Id.* at 13.

and intending to limit, but not preclude, CD copying using computers.²¹ In addition, XCP also contained similar language in its EULA, stating that “the Software will not be used at any time to collect any personal information from you, whether stored on Your Computer or otherwise.”²² However, also like MediaMax, XCP “phone[ed] home to the vendor or record label with information about users’ listening habits despite statements to the contrary from the vendors.”²³ XCP contained a temporary protection measure for the period immediately after inserting the disc that would, when the EULA was presented, essentially freeze the operations on the computer and conduct a search of the hard drive for any running processes that appeared on XCP’s blacklisted programs.²⁴ If it found any of the programs on its blacklist, then it “initiat[ed] a 30-second countdown timer; if any of the applications are still running when the countdown reaches zero, the installer ejects the CD and quits.”²⁵ However, if a user did agree to accept the EULA, “it would not be

While computers sometimes fail to display the EULA after inserting the CD into the drive, thus allowing users to access the music with other media players, “if the consumer inserts the CD and the [Sony] EULA is displayed, the consumer will no longer be able to use these other media players to play the audio CD.” *Texas v. Sony BMG Music Entertainment, LLC*, No. GV505065 (126th Tex. Dist. Ct. Nov. 21, 2005), available at <http://www.oag.state.tx.us/newspubs/releases/2005/112105sonypop.pdf> [hereinafter *Texas Litigation*].

²¹ Rather than inhibit all copying of the discs, “XCP allowed users to make up to three copies of the CD, but tracks could only be played with the media player that was included with the CD and could only be downloaded to certain types of portable players.” LaBelle, *supra* note 14, at 92.

²² XCP, End User License Agreement.

²³ HALDERMAN & FELTEN, *supra* note 9, at 14.

²⁴ *Id.* at 6. XCP contained a list of nearly 200 ripping and copying applications incorporated into its execution program. “If one or more blacklisted applications are running, the installer replaces the EULA display with a warning indicating that the applications need to be closed in order for the installation to continue.” *Id.*

²⁵ *Id.*

displayed again when another CD with XCP software was loaded onto that user's computer. So the user was given just one opportunity to read the [EULA] language."²⁶

Another (more alarming) feature of XCP was that, when the DRM protection was installed, another component, called a rootkit, was also installed on the user's hard drive without notification.²⁷ A rootkit is a tool used for tunneling into and embedding software deep in a computer's operating system to hide the fact that certain processes, files, or system data exist on the computer, thus helping an intruder maintain access without the user's knowledge.²⁸ In addition, "rootkits are created to be extraordinarily difficult to uninstall without specific instructions, rooting themselves in an operating systems' deepest recesses in order to prevent their deletion."²⁹ Upon installation, the Sony rootkit conceals the XCP protection itself (and any other program for that matter) by hiding all programs that begin with the prefix "\$sys\$," making those applications "invisible to normal programs and administration tools."³⁰ Thus, the DRM provides a hiding place for other programs that wish to attack the computer. In this manner, XCP renders a user's

²⁶ LaBelle, *supra* note 14, at 93.

²⁷ The term rootkit "refers to a set of tools that hide any trace of an intruder yet maintain full, or 'root,' access on system running the operating system." Joris Evans, What Makes a Rootkit?, CNET NEWS.COM, Nov. 21, 2005, *available at* http://news.com.com/What+makes+a+rootkit/2100-1029_3-5961568.html.

"The XCP EULA says nothing about this rootkit." LaBelle, *supra* note 14, at 93.

²⁸ John Borland, Sony CD Protection Sparks Security Concerns, CNET NEWS.COM, Nov. 1, 2005, *available at* http://news.com.com/Sony+CD+protection+sparks+security+concerns/2100-7355_3-5926657.html. *See also* BBC NEWS, Sony Sued Over Copy-Protected CDs, Nov. 10, 2005, *available at* <http://news.bbc.co.uk/go/pr/fr/-/1/hi/technology/4424254.stm>. ("Rootkits are being increasingly used by virus makers to hide their malicious wares deep inside the Windows operating system.") *Id.*

²⁹ *Id.*

³⁰ HALDERMAN & FELTEN, *supra* note 9, at 9-10.

computer vulnerable by allowing “Malware authors [to] exploit the fact that any files, registry keys, or processes with names beginning in \$sys\$ will be hidden....”³¹

Suffice it to say, Sony exceeded its legal authority by implementing these two DRM technologies. In response to the public disclosure of its rootkit scandal,³² infuriated consumers from around the world pounced on Sony over its apparent abuse of the Copyright Act.³³ In fact, shortly after the controversy arose, many disgruntled consumers organized a concerted effort to boycott Sony CDs and merchandise.³⁴ The following section examines the various court actions that emerged after the rootkit scandal and analyzes the potential liabilities of both Sony and the affected consumers who attempted to remove the DRM from their computers.

III. LITIGATION AND POTENTIAL LIABILITIES

Numerous lawsuits were brought against Sony on various grounds, most commonly unfair trade practice, consumer fraud, false advertising, and deceptive trade practice laws of many states, the Computer Fraud and Abuse Act (CFAA),³⁵ and various

³¹ *Id.* at 19.

³² See *infra* notes 75-78 and accompanying text.

³³ See Nils’ Weblog About All Things Geek, *Sony Music Installs Rootkit With CD*, GEEK WORLD, Nov. 1, 2005. The rootkit scandal has only confirmed the widespread public perception of corporate greed and corruption associated with record companies, and has served to fuel the cynicism, distrust, and general hatred of these corporate “suits” maintained by many underground consumers. Consequently, many web blogs have been created which call for a realistic and effective penalty for Sony’s conduct, as well as a boycott of all Sony products. *Id.* at *Sony Scandal – Affected CDs, Boycott?*, Nov. 22, 2005.

³⁴ *Id.*

³⁵ CFAA, 18 U.S.C. §§ 1030, *et seq.* (1986).

state and federal common law claims.³⁶ Most of these suits were consolidated into one class action suit (Consolidated Action) in the Southern District of New York, where, in December of 2005, the affected parties reached a settlement with Sony over the litigation.³⁷ One case was brought in Texas, where state Attorney General Greg Abbott filed an action claiming that Sony violated that state's Consumer Protection Against Spyware Act (CPACSA)³⁸ by releasing CDs with XCP software.³⁹ Both of these cases have since settled out of court, but they help identify the legal issues surrounding Sony's conduct and assist in understanding the potential liabilities that Sony exposed itself to by releasing its affected CDs. Another argument may be made that, by limiting the practical uses of its CDs and restricting their playing, copying, and downloading capabilities, Sony infringed the consumers' fair use rights to their legally purchased audio CDs under the *Sony Corp. v. Universal Studios*⁴⁰ and *RIAA v. Diamond Multimedia Systems*⁴¹ doctrines, and thus is in violation of the Copyright Act. On the other hand, the consumers, by attempting to remove the DRM from their computers, may have violated the anti-circumvention sections of the Digital Millennium Copyright Act (DMCA).⁴² Moreover,

³⁶ See, e.g., LaBelle, *supra* note 14, at 99-100; Settlement Agreement P. I. I-M, In re Sony BMG CD Technology Litigation, No. 1:05-cv-09575-NRB (S.D.N.Y. 2005), available at <http://www.sonybmgcdtechsettlement.com/pdfs/SettlementAgreement.pdf> [hereinafter Settlement Agreement]; HALDERMAN & FELTEN, *supra* note 9, at 2. In addition, Sony is the subject of an inquiry by the Federal Trade Commission, as well as several state attorneys general and governmental authorities in various jurisdictions. Settlement Agreement, P. I, M.

³⁷ Settlement Agreement, *supra* note 36, P. I, J-N.

³⁸ CPACSA, TEX. BUS. & COM. CODE § 48.001 *et seq.* (Vernon Supp. 2005).

³⁹ Texas Litigation, *supra* note 20; see also, *infra*, note 52-55 and accompanying text.

⁴⁰ 464 U.S. 417 (1984).

⁴¹ 180 F.3d 1072 (9th Cir. 1999).

⁴² DMCA 17 U.S.C.A. § 1201 *et seq.* (1998).

the researchers from Princeton University, as well as Mark Russinovich, and even the local computer store or technician, may also have violated the DMCA for distributing information related to circumventing the Sony DRM and trafficking technical support designed to erase the software from individuals' computers.

A. Sony's Liability under the CFAA

The CFAA prohibits seven types of conduct related to computer activity, including “intentionally accessing a computer without authorization, or exceeding authorized access, to obtain information”⁴³ and “intentionally accessing a ‘protected computer’ without authorization and causing damage.”⁴⁴ In order to bring a civil lawsuit under the latter of these two CFAA provisions, a plaintiff must show that he or she: 1) suffered damage or loss due to a violation of the statute, to one or more persons during any one year period aggregating at least \$5000 in value, and 2) that the conduct at issue involved one of the factors listed in the statute.⁴⁵ In the Consolidated Action, the plaintiffs relied upon section five of CFAA, which requires plaintiffs to show that Sony intentionally accessed the computers without authorization, and that \$5000 in damages was inflicted upon plaintiffs' computers.⁴⁶ In regard to the first requirement, that the access be unauthorized, plaintiffs could easily satisfy this prong because of the method in which MediaMax was installed on computers.⁴⁷ Since the DRM was installed without consenting to the EULA (sometimes even when the EULA terms were rejected), the computer was certainly accessed without authorization. However, a question remains as

⁴³ 18 U.S.C.A. § 1030 (a)(2).

⁴⁴ *Id.* § 1030 (a)(5).

⁴⁵ *Id.*

⁴⁶ *Id.*

⁴⁷ *See supra* notes 12-14 and accompanying text.

to the minimum damages requirement of the statute: can all plaintiffs in the class consolidate the amount of damage inflicted upon all of their respective computers, or must an individual plaintiff meet the \$5000 alone?⁴⁸ Whatever the answer to that question may be, the parties settled before the suit was litigated, so the success of the action on the merits remains unresolved.⁴⁹

However, the class action suit was based solely upon section five of the CFAA, thus leaving a potentially successful claim based upon the other relevant clause: section two. Section two prohibits conduct or software that “intentionally accesses a computer without authorization or exceeds authorized access, and thereby obtains... information from any protected computer if the conduct involved an interstate or foreign communication.”⁵⁰ Seeing as how the conduct at issue here involved the sale of CDs by an international record label, loading and installing software on computers across the country, in addition to secretly transmitting information back to Sony and the DRM manufacturer,⁵¹ the conduct easily falls within the realm of section two of CFAA. Moreover, since the information was tracked and relayed back to Sony without notice to users, and in direct contrast to the EULA terms, this conduct was undoubtedly unauthorized as far as the statute is concerned. Hence, the likelihood that Sony would be held liable under section two of the CFAA is reasonably substantial under these circumstances.

⁴⁸ The courts are split on the question of whether plaintiffs’ damages in a class action suit can be aggregated for purposes of bringing a claim under § 1030(a)(5) of the CFAA. *See* LaBelle, *supra* note 14, at 103-06.

⁴⁹ *See generally*, Settlement Agreement, *supra* note 36.

⁵⁰ 18 U.S.C. § 1030 (a)(2)(C).

⁵¹ HALDERMANN & FELTEN, *supra* note 9, at 14.

B. Sony's Liability under the Texas CPACSA

In 2005, Texas Attorney General Greg Abbot brought an action against Sony for violating certain provisions of the CPACSA.⁵² Abbott alleges that, because of its rootkit feature, XCP (and only XCP) violated the relevant portion of the act. Under section 48.053 of the CPACSA, the Texas legislature has made illegal:

[The use of] software to change the name, location, or other designation of computer software to prevent the owner from locating and removing the software...and [to] create randomized or intentionally deceptive file names or random or intentionally deceptive directory folders, formats, or registry entries to avoid detection and prevent the owner from removing computer software.⁵³

According to the plaintiff's petition, the XCP cloaking mechanism violates this part of the statute because of the very nature of its intended operation. As alleged by Abbott, "[t]he [rootkit] is not required to play Sony BMG's copy protected CDs; rather its purpose is to conceal the copy protection software installed by Sony BMG."⁵⁴ In doing so, according to Abbott, Sony has knowingly "copied [computer software] to a computer, of which it is not the owner or operator, and used that software to change the name, location or other designation ... and create[d] randomized or intentionally deceptive file names ... to avoid detection and prevent the owner from removing computer software."⁵⁵

⁵² Texas Litigation, *supra* note 20.

⁵³ CPACSA §§ 48.053(5)-(6).

⁵⁴ Texas Litigation, *supra* note 20, at 3-4.

⁵⁵ *Id.* at 6.

In light of the apparent lack of any credible defense,⁵⁶ and based upon a natural reading of the plain language of the statute, it would appear that Sony's XCP DRM clearly violated the Texas anti-spyware statute.⁵⁷ However, after a year of litigation on the matter, Abbot settled with Sony in December of 2006, and Sony has agreed to discontinue the use of XCP and MediaMax for copy protection of CDs.⁵⁸

C. Sony's Liability under the Copyright Act: Fair Use Violation?

Another potential liability for Sony exists in the manner in which its DRM severely restricted (and in some cases precluded) consumers' fair use of their legally purchased audio CDs.⁵⁹ In *Sony Corp. v. Universal Studios*⁶⁰ and *RIAA v. Diamond Multimedia Systems*,⁶¹ the courts have clarified the issue of copying protected materials by individual consumers and making fair use of those copies. In *Sony*, Sony, the manufacturer of VCRs, was sued by Universal Studios, the owner of numerous copyrighted movies and television shows, for providing equipment that allowed copying of plaintiff's copyrighted movies in violation of the Copyright Act. The Supreme Court

⁵⁶ An NPR interview with Thomas Hesse, the President of Sony's Global Digital Business division, reveals that Sony did in fact know about the software's spyware behavior and that it was intentionally cloaked "so would be pirates can't find it and remove it." Interview with Thomas Hesse, NATIONAL PUBLIC RADIO, Nov. 4, 2005, available at <http://www.npr.org/templates/story/story.php?storyId=4989260>.

⁵⁷ For a discussion about a potential constitutional argument based upon the statute's violation of the dormant commerce clause, see LaBelle, *supra* note 14, n. 293.

⁵⁸ Agreed Final Judgment and Permanent Injunction, *Texas v. Sony BMG Music Entertainment*, No. GV505065 (Tex. D.C. 2006). The Court granted a permanent injunction against Sony's use of these DRMs on CDs, which also requires Sony to give "clear and conspicuous" notice of all future uses of copy protection technologies on CDs as well as their possible and realistic effects upon PCs. *Id.*

⁵⁹ For a discussion on the Fair Use argument against the DMCA, see Carol Guess, *Downloading in a Post-Napster World: May Fair Use Be With You*, 44-DEC. HOUS. LAW. 18 (2006).

⁶⁰ 464 U.S. 417 (1984).

⁶¹ 180 F.3d 1072 (9th Cir. 1999).

held that Sony did not violate the Copyright Act by providing VCRs to the general public and established that “time shifting,” the recording of copyrighted materials for personal use at a later time, is an accepted fair use of otherwise protected works.⁶² Fifteen years later, the Ninth Circuit held in *Diamond* that a portable mp3 player was not a digital audio recording device under the Audio Home Recording Act (AHRA)⁶³ because it could not itself reproduce the digital content onto another source.⁶⁴ The court went on to carve out another fair use exception for copying protected works, holding that “the Rio merely makes copies in order to render portable, or ‘space-shift,’ those files that already reside on a user’s hard drive.”⁶⁵ The court emphasized that “[s]uch copying is paradigmatic noncommercial personal use entirely consistent with the Copyright Act.”⁶⁶

It is clear, then, that courts generally deem the copying of legally purchased copyrighted materials for private, noncommercial use as a fair use exception to the Copyright Act. Therefore, the greater the limitations that restrict users’ abilities to space and time shift their audio files are, the more those restrictions resemble an infringement of those users’ fair use rights. Because this is a relatively novel issue, it remains uncertain whether the DRM incorporated on Sony CDs would be deemed an infringement of consumers’ fair use rights. Neither of the Sony DRM programs totally precluded

⁶² 464 U.S. at 451-56. The Court held that, because time shifting does not adversely affect the market for plaintiff’s television shows and movies, and since it is a non-commercial, personal use by the user, “home time-shifting is fair use.” *Id.* at 455.

⁶³ 17 U.S.C.A. § 1001 *et seq.* (1992). The AHRA prohibits copyright owners from bringing infringement actions against consumers of digital audio equipment that permits noncommercial, private recording of copyrighted works. *Id.* 17 U.S.C.A. § 1008.

⁶⁴ 180 F.3d at 1077-81.

⁶⁵ *Id.* at 1079.

⁶⁶ *Id.*

making copies of the CD tracks,⁶⁷ but they did restrict users from copying them onto most mp3 players, and they severely limited the users' abilities to play the CDs on their personal computers.⁶⁸ Although the copying of these CDs is most likely a private, noncommercial use that probably qualifies for the *Diamond* fair use exception, this fact, alone, will probably not make a successful argument in court.⁶⁹ More likely, rather, “[unless] DRM continues to ravage personal computers the way [Sony’s] has,” as many scholars have noted, “Courts are likely to rule that DRM does not violate a purchaser’s Fair Use of CDs in this scenario.”⁷⁰

D. Consumer and Researcher Liabilities under the DMCA

The anti-circumvention provisions of the DMCA prohibit a person from “circumventing a technological measure that effectively controls access to a work protected under the Copyright Act.”⁷¹ In addition, under the DMCA:

No person shall manufacture, import, offer to the public, provide, or otherwise traffic in any technology, product, service, device...that is primarily designed or produced for the purpose of circumventing protection afforded by a technological measure that effectively protects a right of a copyright owner under this title in a work or a portion thereof.⁷²

⁶⁷ HALDERMANN & FELTEN, *supra* note 9, at 13-14. They permitted a user to make up to three copies of an affected CD.

⁶⁸ *Id.*

⁶⁹ *See* Guess, *supra* note 59, at 16-18.

⁷⁰ *Id.* at 16. In fact, the Second Circuit has stated that “the Supreme Court has never held that fair use is constitutionally required.” *Universal Studios v. Corley*, 273 F.3d 429, 458 (2d Cir. 2001).

⁷¹ 17 U.S.C.A. § 1201(a)(1)(A).

⁷² *Id.* § 1201 (a)(2)(b).

These provisions create a dilemma for the customers whose computers were affected by Sony's DRM: do users who remove Sony's spywareish DRM violate the DMCA? For that matter, do the computer technicians who assist in reprogramming an affected PC and the researchers who provide information on how to uninstall it also violate the DMCA?

On its face, it appears that these efforts do violate the basic terms of the statute: users are circumventing Sony's copy-prevention technologies. However, the DMCA also establishes two particular exceptions to the prohibited conduct under which these users would likely be sheltered from liability. The first provision, section 1201(i), creates an exception for users who circumvent the technological measures in an effort to protect personally identifying information.⁷³ Since both XCP and MediaMax contained "phone home" functions that transmitted personal information related to the users' PCs, a user who removed the DRM from their computer would probably be sheltered by section 1201(i). The second provision that would apply is section 1201(j), which allows users to remove the DRM in a good faith effort to investigate and test the computer for security vulnerabilities and breaches.⁷⁴ Since XCP exposed affected computers to any number of viruses that a hacker was willing to impose, and MediaMax often installed itself without

⁷³ 17 U.S.C.A. § 1201(i). The statute says that:

It is not a violation ... for a person to circumvent a technological measure that effectively controls access to a work protected under this title if the technological measure, or the work it protects, contains the capability of collecting or disseminating personally identifying information reflecting the online activities of a natural person who seeks to gain access to the work protected.

Id.

⁷⁴ 17 U.S.C.A. § 1201(j). The statute defines security testing as "accessing a computer, computer system, or computer network, solely for the purpose of good faith testing, investigating, or correcting, a security flaw or vulnerability, with the authorization of the owner or operator of such computer, computer system, or computer network." *Id.*

consent, a user's attempts to correct the security flaws presented by these programs would most likely also fall into this exception to the prohibited conduct of the DMCA.

When Mark Russinovich, an experienced computer programmer, discovered a rootkit on his computer in 2005, he traced its presence to a Sony CD he recently uploaded onto his computer.⁷⁵ After his discovery and removal of the program, he published a detailed account of his findings online, along with sharp criticism of Sony's DRM tactics.⁷⁶ Shortly after this publication, John Halderman and other researchers at Princeton University conducted an in-depth examination of Sony's CDs and released findings on the internal processes of XCP and MediaMax in their university journal.⁷⁷ Thus, it would appear that, under the plain language of the DMCA, these researchers have violated the anti-trafficking provision of the statute. They each provided detailed information about the technologies used to protect copyrighted recordings and described how those technologies could be removed from computers.⁷⁸ However, while it still remains an uncertainty, under the "good faith research and testing" exception described above, it is arguable that these researchers would also have been shielded from liability for violation of the statute.

IV. RECENT DEVELOPMENTS AND THE GOVERNMENT'S RESPONSE TO SONY'S DRM

⁷⁵ Borland, *supra* note 28.

⁷⁶ *Id.*

⁷⁷ *See generally*, HALDERMAN & FELTEN, *supra* note 9.

⁷⁸ *See id.*; *see also* Borland, *supra* note 28.

After the Sony DRM debacle exploded in 2005, significant efforts to change the structure of the interrelation between the Copyright Act and the DMCA were initiated. For example, in 2006, upon recommendation of the Register of Copyrights (and as a direct response to the Sony incident), the Library of Congress added an exemption to the anti-circumvention violations of the DMCA.⁷⁹ The new class of exemptions is:

Sound recordings, and audiovisual works associated with those sound recordings, distributed in compact disc format and protected by technological protection measures that control access to lawfully purchased works and create or exploit security flaws or vulnerabilities that compromise the security of personal computers, when circumvention is accomplished solely for the purpose of good faith testing, investigating, or correcting such security flaws or vulnerabilities.⁸⁰

While this class has not yet been incorporated into the DMCA, it is nevertheless an active exemption to the DMCA violations for the next three years or until Congress formally amends the DMCA and includes the provision in the statute.⁸¹ Therefore, it does take a step in the direction of protecting individuals' fair use of copyrighted material in accordance with the *Diamond* rule,⁸² albeit a small step.

In addition to this new rule issued by the Librarian of Congress, a bill is currently going through Congress that would officially recognize the fair uses of copyrighted

⁷⁹ Copyright Office, Rulemaking on Exemptions from Prohibition on Circumvention of Technological Measures that Control Access to Copyrighted Works, *available at* <http://www.copyright.gov/1201/index.html>.

⁸⁰ *Id.* at 6.

⁸¹ Statement of the Librarian of Congress Relating to Section 1201 Rulemaking, *available at* http://www.copyright.gov/1201/docs/2006_statement.html.

⁸² *See supra* notes 65-66 and accompanying text.

works in legislation. The bill, The Freedom and Innovation Revitalizing U.S. Entrepreneurship Act of 2007 (Fair Use Act),⁸³ would essentially “limit the amount of control that content owners are granted by copyright laws over their work.”⁸⁴ If enacted, the Act would accomplish three main goals: 1) limit the availability and amount of statutory damages for secondary liability; 2) limit the rigidity and strength of the DMCA by adding twelve additional exemptions; and 3) resolve the *Sony-Betamax* quagmire, officially “making clear that manufacturers cannot be held liable based on the design of technologies with substantial non-infringing uses.”⁸⁵

However, despite the grandiose projections of the bill’s sponsors, many critics attack the Act for its shortsightedness and ultimate futility, and classify it as “almost entirely symbolic.”⁸⁶ In wanting to reform the DMCA in order to increase leniency, the Act advances idealistic notions and good intentions, but that is all. For example, the bill exempts users of software that provides access to copyrighted works, but offers no protections for the developers of that software. According to one critic, “[the Act is] rendered toothless by the fact that [the exemptions] apply only to the act of circumvention itself, *not* to the act of ‘trafficking’ in tools that would enable non-

⁸³ H.R. 1201, 110th Cong., 1st Sess. (2007).

⁸⁴ Government May Relax Copyright Law For Educational Purposes, DAILY KENT STATER, Mar. 12, 2007, *available at* <http://media.www.stateronline.com/media/storage/paper867/news/2007/03/12/OtherCampuses/Government.May.Relax.Copyright.Law.For.Educational.Purposes-2772103.shtml>.

⁸⁵ Support the Fair Use Act of 2007, ELECTRONIC FRONTIER FOUNDATION, *available at* <https://secure.eff.org/site/Advocacy?JServSessionIdr008=ftj3xu49x3.app2a&cmd=display&page=UserAction&id=271>.

⁸⁶ Tim Lee, Fair Use Act Analysis: DMCA Reform Left on the Cutting Room Floor, ARS TECHNICA, Feb. 28, 2007, *available at* <http://arstechnica.com/news.ars/post/20070228-8942.html>.

programmers to take advantage of them.”⁸⁷ Consequently, even if enacted, the Act will provide only limited protection to those that it is intended to benefit, and eventually the congressional concern over the Sony scandal will be buried in time and forgotten, resulting in absolutely no useful substantive change or effective punishment for Sony.

V. CONCLUSION

In light of the relatively fluid and speculative nature of the legislative efforts to provide greater protection for fair users of copyrighted works, their general effectiveness and ultimate outcome remains unclear. However, in a contemporary society where online music piracy is an ever-present threat to record companies, and seeing as how DRM technologies continue to be the most effective tool in combating that piracy, it is unlikely that it will go away any time soon. The distressing element about this fact is that DRM use only loosely adheres to the principles of copyright law.⁸⁸ In fact, “[t]he [DRM] systems make no pretense of enforcing copyright law as written, but instead seek to enforce rules dictated by the label’s and vendor’s business models.”⁸⁹ This raises questions about the propriety of the sweeping scope of protection currently provided by the Copyright Act: what are the interests really being protected here? In light of Sony’s conduct, the interests of the record label appear to be less concerned with content and more concerned with profits. They certainly don’t appear to be engaged in the consumers’ interests.

⁸⁷ *Id.*

⁸⁸ “The design of DRM systems is driven strongly by the incentive of the content distributor and the DRM vendor...and the DRM design will not necessarily serve the interests of copyright owners.” HALDERMAN & FELTEN, *supra* note 9, at 26.

⁸⁹ *Id.*

Whatever their interests may be, and regardless of the prohibitions imposed by the DMCA, courts have held that “consumers who purchase a product containing a copy of embedded software have the inherent legal right to use that copy of the software.”⁹⁰ In addition, the “statutory structure and the legislative history both make it clear that the DMCA granted copyright holders additional legal protections, but neither rescinded the basic bargain granting the public noninfringing and fair uses of copyrighted materials... nor prohibited various beneficial uses of circumvention technology, such as those exempted under §§1201(d),(f),(g),(j).”⁹¹

⁹⁰ Chamberlain Group, Inc. v. Skylink Tech., 381 F.3d 1178, 1202 (Fed. Cir. 2004).

⁹¹ *Id.*