Denver Law Review

Volume 84 | Issue 1 Article 5

December 2020

# The Rootkit Debacle: The Latest Chapter in the Story of the Recording Industry and the War on Music Piracy

Megan M. La Belle

# THE "ROOTKIT DEBACLE": THE LATEST CHAPTER IN THE STORY OF THE RECORDING INDUSTRY AND THE WAR ON MUSIC PIRACY

MEGAN M. LABELLE†

ABSTRACT

*In the age of digital music, illicit copying or burning of CDs is a rampant problem that undermines the rights of copyright holders, record labels, and artists alike. The recording industry has attempted to address this problem by manufacturing and releasing CDs with various types of digital rights management (DRM) technologies. Most recently, Sony BMG introduced CDs containing DRM software that was intended, among other things, to limit the number of copies of the CD the user could make, and prevent the user from sharing the content of the CD on peer-to-peer networks. However, the manner in which this software operated was highly controversial, for example because it collected information from the user's computer and installed a "rootkit" on the user's hard drive that made the computer susceptible to viruses. This latest effort to copy-protect CDs, which has come to be known as the "rootkit debacle," has raised numerous legal issues that are examined in this article, including Sony BMG's potential liability under certain federal and state laws, as well as the potential liability of consumers and security researchers under the Digital Millennium Copyright Act. The article also proposes a solution for striking a balance between the recording industry's right to protect its intellectual property and music fans' right to enjoy their CDs.*

TABLE OF CONTENTS



† Megan M. LaBelle is a commercial litigator whose practice focuses on intellectual property, and she is an adjunct professor at The Catholic University of America Columbus School of Law. Ms. LaBelle is a graduate of the University of California, Los Angeles (B.A. *summa cum laude*) and the University of California, Davis School of Law (J.D. Order of the Coif).

## INTRODUCTION

Over the past decade, the recording industry's war on piracy has focused on music downloaded from the Internet and file sharing. As a result of recent court victories, the recording industry now appears to have the upper hand in the on-line file sharing battle. While this battle certainly is not over, this respite has given the record labels an opportunity to focus on another alleged culprit in the struggles of the music business: the copying or "burning" of compact discs (CDs).

The recording industry is well aware of the impact that burned CDs have had on its business. As one industry leader said, "[m]usic copied onto blank recordable CDs is becoming a bigger threat to the bottom line of record stores and music labels than online file-sharing."[1] Indeed, for several years now, the major music labels have been experimenting with digital rights management (DRM) and other anti-piracy technologies that, among other things, would prevent consumers from converting their CDs into computer files, limit the number of copies of a CD a consumer could make, and/or render CDs unplayable on certain types of audio equipment.

Nevertheless, until recently, discussions about whether CDs included DRM were reserved for Internet bloggers, outspoken consumer groups, and serious music fans. In 2005, that all changed when Sony BMG (Sony) released dozens of albums by popular artists with DRM software installed on the CD.[2] The purpose of this software was to thwart music piracy and protect Sony's intellectual property, while at the same time providing customers with flexibility in playing their music. Specifically, the software allowed customers to make up to three copies of the CD and play the content on multiple platforms, while attempting to prevent excessive copying and sharing of music on peer-to-peer websites.[3]

---

1. *Copying Music Now Threatens Business Like File-Sharing Did*, ASSOCIATED PRESS (New York), Aug. 15, 2005, at 12.

2. *See Sony Tests Technology to Limit CD Burning*, REUTERS, June 1, 2005, http://news.cnet.co.uk/digitalmusic/0,39029666,39189658,00.htm; *see also* Wikipedia, 2005 Sony CD Copy Protection Scandal §1, http://en.wikipedia.org/wiki/2005_Sony_CD_copy_protection_controversy (last visited Sept. 8, 2006).

3. *Id.*

Although Sony claims its copy-protected CDs contained warnings, most consumers did not become aware of the software until after they had purchased the CDs. To exacerbate matters, the software worked by secretly installing a "rootkit" on a purchaser's hard drive when the purchaser first loaded the CD on a drive connected to a computer. These rootkits exposed the users' computers to hackers who could introduce viruses and then exploit those viruses to their advantage. Moreover, the software, which opponents claim is spyware, kept track of what consumers did with the purchased music and then communicated that information back to Sony.[4]

In early November 2005, the news of Sony's DRM software exploded on the Internet and, soon thereafter, Sony pulled approximately fifty titles from retail stores.[5] Though some people find DRM inherently objectionable, the widespread outrage may have had more to do with the manner in which the software operated than with the purposes it served. In any event, Sony's use of this specific DRM tool has disillusioned consumers, lawmakers, and artists alike. Consequently, several consumer class action lawsuits and one law enforcement action have been filed against Sony.[6] Settlements have now been reached in many of these cases, and Sony has agreed, among other things, to replace CDs containing DRM software with unprotected versions and to stop using the specific type of DRM software at issue in these lawsuits.[7]

But this is not the end of the story. The "rootkit debacle" has raised numerous legal questions that remain unanswered. These questions are sure to rear their heads again, especially given that Sony and the other record labels have made clear that they are not abandoning future efforts to protect CDs from unfair copying. This article attempts to resolve these unanswered questions.

Part I of this article provides a background of the recording industry's war against music piracy over the past several years. Part II describes Sony's latest effort to copy-protect CDs, which has become

---

4. Mark Russinovich, *Sony, Rootkits and Digital Rights Management Gone Too Far*, SYSINTERNALS BLOG, Oct. 31, 2005, http://www.sysinternals.com/blog/2005/10/sony-rootkits-and-digital-rights.html; Mark Ward, *Sony's Music Arm Has Been Accused of Using the Tactics of Virus Writers to Stop its CDs Being Illegally Copied*, BBC.com, http://news.bbc.co.uk/2/hi/technology/4400148.stm; Matthew Fordahl, *Sony to Offer Patch To Reveal Hidden Copy-protection Software*, ASSOCIATED PRESS (San Jose, Calif.), Nov. 12, 2005.

5. *Sony-BMG Flushes DRM Down the Toilet*, SILICON VALLEY SLEUTH, Nov. 15, 2005, http://www.siliconvalleysleuth.com/2005/11/sonybmg_flushes.html.

6. *Sony Sued Over Copy-protected CDs*, BBC.com, Nov. 10, 2005, http://news.bbc.co.uk/2/hi/technology/4424254.stm; Sony BMG CD Technologies Settlement, Apr. 7, 2006 (last updated), http://www.sonybmgcdtechsettlement.com.

7. *See* Sony BMG, Important Legal Notices/Software Update Notice, http://cp.sonybmg.com/xcp (last visited Sept. 15, 2006). "If You Bought, Received or Used a SONY BMG Music Entertainment CD Containing Either XCP or Media Max Content Protection Software, Your Rights May Be Affected By a Class Action Settlement, And You Should Download Updates For That Software." *Id.*

known as the "rootkit debacle." Part III analyzes the legal questions raised by the Sony rootkit debacle, including whether: (i) Sony violated certain anti-fraud and spyware-related laws by distributing CDs with copy-prevention software; (ii) Sony's copy-protected CDs comported with copyright law, namely the fair use doctrine; and (iii) consumers' removal of the copy-prevention software or distribution of information about how to remove such software violated the Digital Millennium Copyright Act. Finally, Part IV proposes a solution that attempts to strike a balance between the recording industry's right to protect its intellectual property and a consumer's right to enjoy purchased music.

## I. BACKGROUND: THE MUSIC INDUSTRY'S WAR ON PIRACY

Less than ten years ago the music business was booming. In 1999, CD sales totaled $14.6 billion with approximately 1.5 billion units shipped worldwide.[8] The business grew at an annual rate of greater than 6 %, and everyone involved made a lot of money.[9]

Since 1999, the recording industry has experienced a serious downward trend. By 2003 the number of units shipped was down 31 %,[10] and CD sales had fallen to $11.2 billion.[11] Consequently, in an effort to save money, record labels have laid off employees, ditched artists, cut tour and video budgets, and reissued old albums rather than produce and promote new ones.[12] While numerous factors have contributed to this decline, the major culprit is music piracy—both in the form of file sharing and CD burning.[13] Thus, over the past several years, the recording industry has invested significant time and resources waging war against these pirates in an attempt to regain the success it once enjoyed.

---

8. Jefferson Graham et al., *Hammering Away at Piracy*, USA TODAY, Sept. 11, 2003, at 1D; NARM Consumer Research Initiative Phase One: Consumer Profiles & Retail Experience, Prepared for: National Association of Recording Merchandisers, Mar. 2006, at 11, *available at* http://www.slyck.com/misc/NARMNPDStudy0603.pdf#search=%22NARM%20Consumer%20Research%20Initiative%20Phase%20One%3A%20Consumer%20Profiles%20%26%20Retail%20Experience%22 [hereinafter NARM].

9. Graham et al., *supra* note 8, at 1D.

10. NARM, *supra* note 8, at 11.

11. Kristina Groennings, *Costs & Benefits of the Recording Industry's Litigation Against Individuals*, 20 BERKELEY TECH. L.J. 571, 573 (2005).

12. Hillary M. Kowalski, *Peer-to-Peer File Sharing & Technological Sabotage Tactics: No Legislation Required*, 8 MARQ. INTELL. PROP. L. REV. 297, 301 (2004); David Segal, *A New Tactic in the Download War: Online "Spoofing" Turns the Tables on Music Pirates*, WASH. POST, Aug. 21, 2002, at A1.

13. Some have blamed the decline in record sales on the nation's economic downturn. *See* Peter K. Yu, *P2P & the Future of Private Copying*, 76 U. COLO. L. REV. 653, 765 n.15 (2005). Others contend that people are buying less music because they have so many other entertainment options. *See* NARM, *supra* note 8, at 16.

### *A. The First Phase: On-Line File Sharing*

#### 1. The Battle Against Indirect Infringers

Thus far, the recording industry's war on piracy has focused primarily on indirect infringers, *i.e.*, companies whose products facilitate the downloading and file sharing of copyrighted music. The most well known of these alleged indirect infringers was Napster, a peer-to-peer file sharing service that utilized a centralized index of music files and allowed those files to be transferred from one Napster user's computer to another.[14] Napster's emergence in late 1999 coincided with the sharp decline in CD sales. The Recording Industry Association of America ("RIAA") responded on behalf of its members by suing Napster on the grounds of contributory and vicarious copyright infringement.[15] After years of protracted litigation, the RIAA defeated Napster, ultimately forcing it into bankruptcy.[16]

Although the Napster litigation was a success for the recording industry, it did not put an end to on-line file sharing. Instead, Napster users migrated to decentralized file sharing services such as Grokster.[17] Such services did not have a centralized index like Napster, but rather, distributed software that allowed users to share electronic files through peer-to-peer networks.[18] In 2001, the RIAA filed suit against Grokster and StreamCast Networks, another software distributor, asserting the same theories as in the *Napster* case.[19] The district court granted summary judgment in favor of the software companies because (i) their software was capable of substantial non-infringing use, and (ii) they had no actual knowledge of infringement by their customers.[20] The Ninth Circuit affirmed.[21]

The United States Supreme Court granted certiorari in the *Grokster* case and reversed.[22] In so doing, the Court found that close to 90% of

---

14. Mark F. Radcliffe & Jill Sazama, *Napster & Hollywood: Controlling Intellectual Property in an Age of Peer-to-Peer File Sharing and Digital Video Recorders*, Georgetown Univ. Law Ctr. CLE, 2002 WL 32152238, at *2 (Nov. 14-15, 2002).

15. *See* Complaint for Contributory and Vicious Copyright Infringement at 2, A&M Records, Inc. v. Napster, Inc., 114 F. Supp. 2d 896 (N.D. Cal. 2000), *affirmed by* 239 F.3d 1004 (9th Cir. 2001) *available at* http://www.riaa.com/news/filings/pdf/napster/Napster_Complaint.pdf. Soon after it sued Napster, the recording industry also brought a lawsuit against MP3.com, which had launched "myMP3.com," a service that allowed users to play songs that the users "owned" from MP3.com's servers. Radcliffe & Sazama, *supra* note 14, at *2. However, MP3.com did not have the consent of the copyright owners to make these copies or provide this service. *Id.* The record labels and other copyright owners were granted injunctive relief against MP3.com and the cases were quickly settled. *Id.*; *see generally* RIAA, http://www.riaa.com/news/filings/mp3com.asp (last visited Sept. 15, 2006).

16. *Napster, Inc.*, 114 F. Supp. 2d at 899. In 2003, Napster was re-launched as a legal, subscription-based on-line music store. *See* Yu, *supra* note 13, at 669-70.

17. Groennings, *supra* note 11, at 573.

18. *Id.*

19. MGM Studios, Inc. v. Grokster, Ltd., 259 F. Supp. 2d 1029, 1031 (C.D. Cal. 2003).

20. *Grokster*, 259 F. Supp. 2d at 1041-43.

21. MGM Studios, Inc. v. Grokster, Ltd., 380 F.3d 1154, 1157 (9th Cir. 2004).

22. MGM Studios, Inc. v. Grokster, Ltd., 125 S. Ct. 2764, 2270 (2005).

the files downloaded with defendants' software were copyrighted.[23] The Court further found that defendants promoted their software as an alternative to Napster, and thus, encouraged users to engage in infringing activity.[24] Accordingly, the Supreme Court held that the software companies were liable for their customers' infringement, reversed the summary judgment, and remanded for further proceedings.[25] As a result of the Supreme Court's decision, the parties settled the case and Grokster was shut down.[26]

2. The Battle Against Direct Infringers

In August 2003, the music industry made the bold and controversial decision to bring copyright suits against direct infringers, *i.e.*, individuals who engage in music downloading and file sharing. For the most part, the RIAA filed these suits against individuals who were heavy users, meaning they had distributed more than a thousand music files on peer-to-peer networks.[27] As of February 2006, approximately 17,765 of these individual copyright infringement lawsuits had been filed.[28]

The media, public, and legal commentators have been highly critical of this litigation strategy, for example because the RIAA has sued college students, deceased persons, and a family that did not own a computer.[29] It is clear, however, that these lawsuits have raised public awareness of the illegality of music downloading and file sharing. Moreover, studies indicate that the user bases of those services that have been targets of the litigation (*e.g.*, KaZaa and Morpheus) have decreased dramatically since the RIAA started its campaign in 2003.[30]

3. Technological Measures

In addition to filing lawsuits, the recording industry has utilized various technological measures to battle individual downloaders and file sharers. The most effective, and perhaps most controversial, of these is

23. *Grokster*, 125 S. Ct. at 2772.

24. *Id.* at 2773.

25. *Id.* at 2782-83.

26. *See* RIAA, http://www.riaa.com/news/newsletter/110705_2.asp (last visited Sept. 15, 2006). The settlement includes a permanent injunction against the software companies prohibiting direct or indirect infringement of any copyrighted works. The injunction also requires the software companies to cease distributing their products and operating their systems. *Id.*

27. Yu, *supra* note 13, at 666.

28. RIAA site, http://www.riaa.com/news/newsletter/default.asp (last visited Sept. 15, 2006).

29. Groennings, *supra* note 11, at 590-91; Yu, *supra* note 13, at 660-61; RIAA website, http://www.riaa.com (last visited Sept. 25, 2006); Anders Bylund, *RIAA Sues Computer-Less Family, 234 Others, for File-Sharing*, ARS TECHNICA, Apr. 24, 2006, http://arstechnica.com/news.ars/post/20060424-6662.html.

30. NARM, *supra* note 8, at 14. However, some studies show that "though litigation caused a decrease in the use of networks . . . targeted by the lawsuits, overall file-sharing has remained unchanged, as users of those sites simply migrated to more secure and anonymous file-sharing systems." Groennings, *supra* note 11, at 587; *see also* Thomas Karagiannis et al., *Is P2P Dying or Just Hiding?*, GLOBAL INTERNET AND NEXT GENERATION NETWORKS, Nov. 2004, at 1, 6, http://www.caida.org/publications/papers/2004/p2p-dying/.

"spoofing." Spoofing is a technique whereby the record industry inserts decoy music files into peer-to-peer networks, thus forcing file sharers to differentiate between the genuine and "fake" files.[31] Some of these "fake" files contain high-pitched screeching sounds, long silences, or repeated loops of the song's chorus.[32] Others contain a message from the artist reminding the file sharer that unauthorized downloading is illegal and harms, not only the record companies, but the artists as well.[33]

Another tactic that reportedly has been used is interdiction.[34] Music companies flood peer-to-peer networks with false requests in order to clog up the network, thereby denying other users the ability to access and download music files.[35] The hope is that peer-to-peer users ultimately will get frustrated enough to stop using these services, and will switch to a legitimate site like iTunes or will purchase the CD at a retail outlet.[36]

### *B. The Second Phase: CD Copying or "Burning"*

#### 1. Identifying the Problem

Unlike the on-line file sharing battle, the recording industry has not engaged in any sort of litigation campaign, either against indirect or direct infringers, to stop individuals from copying CDs from friends or acquaintances. The reasons for this are simple. There are no secondary infringers like Napster or Grokster assisting these individuals in copying CDs; all these individuals need is a borrowed CD and a computer.[37] Fur-

---

31. Sue Zeidler, *Music Labels Plant Online Decoys, Mull Lawsuits*, ELECTRONIC MUSICIAN, July 5, 2002, http://emusician.com/news/emusic_music_labels_plant/index.html; Katie Dean, *Academics Patent P2P Spoofing*, WIRED NEWS, May 8, 2004, http://www.wired.com/news/digiwood/0,1412,63384,00.html.

32. Groennings, *supra* note 11, at 593.

33. *Id.*; Yu, *supra* note 13, at 726-27.

34. Kowalski, *supra* note 12, at 303; Dean, *supra* note 31; Karagiannis et al., *supra* note 30, at 6.

35. Kowalski, *supra* note 12, at 303; Dean, *supra* note 31.

36. Other technological measures that have been contemplated include a program called a "freeze" and a program called a "silence." Kowalski, *supra* note 12, at 302-03.

37. Because of the digital format, copying CDs, unlike records or cassettes, can be accomplished quickly and easily and result in a very high quality duplicate. *See, e.g.*, Amy K. Jensen, *Copy Protection of CDs: The Recording Industry's Latest Attempt at Preventing the Unauthorized Digital Distribution of Music*, 21 J. MARSHALL J. COMPUTER & INFO. L. 241, 244 (2003). CDs can be copied on any computer with a CD-ROM or on a digital audio recording device, *i.e.*, a CD burner or CDR. In 1992, however, Congress passed the Audio Home Recording Act of 1992 (AHRA), Pub. L. No. 102-563, 106 Stat. 4237 (codified at 17 U.S.C.A. §§ 1001-1010 (West 2006)), which "prohibits legal actions for copyright infringement based on the manufacture, importation, or distribution of digital audio equipment or media for private, noncommercial recording." Yu, *supra* note 13, at 706; *see also* Jennifer Norman, *Staying Alive: Can the Recording Industry Survive Peer-to-Peer?*, 26 COLUM. J.L. & ARTS 371, 380 (2003). The AHRA also prohibits infringement actions against the consumers of these products as long as they are being used for a noncommercial purpose. 17 U.S.C.A. § 1008. In exchange, the AHRA requires manufacturers of these products to pay compensatory royalties to copyright holders, 17 U.S.C.A. § 1003(a), and mandates that all such products include a Serial Copy Management System, which limits copying. 17 U.S.C.A § 1002(c).
In light of the AHRA, it would be particularly difficult for the recording industry to bring a lawsuit against the manufacturers and users of CD burners unless it could show that the equipment was not being used for private or noncommercial purposes. In any event, most people today copy CDs on

thermore, based on past experience, the recording industry has realized that suing the manufacturers of computers for contributory infringement is unlikely to advance their cause.[38]

Nor has the RIAA launched a litigation campaign against individuals who copy CDs as it has against on-line file sharers because it would be extremely difficult, if not impossible, to identify these people. The RIAA tracks on-line infringers by their numerical IP address, files a "Doe" lawsuit using that IP address, and then subpoenas the internet service provider (ISP) to obtain the subscriber's identifying information.[39] By contrast, the RIAA has no way of knowing when someone borrows a CD from his friend, copies it onto his hard drive, and then downloads it onto a blank CD or MP3 player.

Yet the recording industry is well aware of the danger posed by these CD burners.[40] Record executives have long argued that CD burning has become so widespread in Europe that it is a bigger threat than unauthorized online file sharing.[41] And a recent study prepared for the National Association of Recording Merchandisers (NARM), a trade organization that represents the interests of major music retailers, indicates that this also may be true in the United States.[42] The study shows that, in 2004, only 43% of fans acquired their music by purchasing a physical CD, while 29% copied a CD, 22% used an illegal peer-to-peer network,

---

their computers, not with a CD burner, and it has been determined that the AHRA does not apply to computers. *See* Recording Indus. Ass'n of Am. v. Diamond Multimedia Sys. Inc., 180 F.3d 1072, 1081 (9th Cir. 1999).

38. In *Sony Corp. of America v. Universal City Studios, Inc.*, 464 U.S. 417, 442 (1984), the Supreme Court held that, even though defendants were aware VCRs were being used to commit infringement, the sale of VCRs could not give rise to contributory infringement because the VCR was capable of commercially significant noninfringing uses, namely time-shifting. Here, manufacturers of computers and CDRs could similarly prove that their products are capable of commercially significant noninfringing uses, and thus, any lawsuit against them is likely to fail. *See id.*

39. Groennings, *supra* note 11, at 574. This is a much more tedious process than the RIAA initially used. *Id.* at 573. When the RIAA first started filing these individual lawsuits, it relied on the subpoena power of § 512(h) of the Digital Millennium Copyright Act (DMCA). *Id.* at 574. Under § 512(h), *before* filing the lawsuit, the RIAA could provide the ISP with "$35, a copy of notification, the proposed subpoena, and a sworn declaration that the information sought was for the sole purpose of protecting copyright," and the ISP was compelled to disclose the subscriber's identifying information. *Id.* However, in *RIAA v. Verizon Internet Services, Inc.*, 351 F.3d 1229, 1237 (D.C. Cir. 2003), the D.C. Circuit Court of Appeals held that ISPs like Verizon are not subject to the subpoena power of § 512(h) because the statute "does not authorize the issuance of a subpoena to an ISP acting as a mere conduit for the transmission of information sent by others." *Id.* Thus, ISPs fall under the safe harbor provision of the DMCA, and copyright holders cannot force them to provide subscriber information without first filing a lawsuit. *Id.* at 1236.

40. *Copying Music Now Threatens Business Like File-Sharing Did*, *supra* note 1, at 12.

41. Jon Healey & Jeff Leeds, *Record Labels Grapple with CD Protection*, L.A. TIMES, Nov. 29, 2002, 3, at 1; *see also Sony's 'Copy-Proof' CD Fails to Silence Hackers*, USA TODAY, May 20, 2002, *available at* http://www.usatoday.com/money/tech/2002-05-20-copyproof-cd.htm (stating that Germany is "rife with illegal CD burning").

42. NARM, *supra* note 8, at 12. This study was prepared by the NPD group, a research organization based in New York that is concerned with the digital music market. *See* Thomas Mennecke, *Is the Physical CD Still a Viable Market?*, Mar. 15, 2006, http://www.slyck.com/news.php?story=1125.

and 6% used legitimate on-line music sites.[43] Therefore, the recording industry has taken a different approach to try to stop illegal copying of CDs: digital rights management.

2. Digital Rights Management: The Solution to CD Burning?

Digital rights management (DRM) is a technology used to protect ownership of digital content by restricting the actions an authorized recipient may take with respect to that content.[44] In other words, DRM systems include "secure packaging and delivery software designed to prevent purchasers and third parties from making unauthorized uses of digital works."[45]

For years, the recording industry has been attempting to prevent or limit unauthorized copying by producing CDs with an effective DRM system. So far, however, those attempts have been unsuccessful.[46] In 2000, for example, the Secure Digital Music Initiative (SDMI), an international organization of record labels, hardware manufacturers, and software manufacturers, challenged computer programmers and researchers to break the digital audio watermark technologies they had developed to prevent the unauthorized copying of CDs.[47] "Digital watermarks contain data, such as copyright information, that identifies a work and is incorporated into the work itself; watermarking allows the content owner to track the use of his work and ensure payment."[48]

Edward Felten, a professor of computer science and public affairs at Princeton University, participated in the contest.[49] Professor Felten's team was able to remove the watermark within just a few weeks, which proved embarrassing for the recording industry.[50] To make matters worse, when Professor Felten attempted to present his findings about the watermark at a conference in 2001, the RIAA and SDMI threatened to

---

43. NARM, *supra* note 8, at 12.

44. Austin Russ, *Digital Rights Management Overview*, SECURITY ESSENTIALS, VOL. 1.2e (July 2001), *available at* http://www.sans.org/reading_room/whitepapers/basics/434.php.

45. Dan L. Burk & Julie E. Cohen, *Fair Use Infrastructure for Rights Management Systems*, 15 HARV. J. L. & TECH. 41, 48 (2001).

46. The film industry, too, has experienced problems with its use of DRM on digital video discs (DVDs). In the 1990s, it developed the Content Scrambling System (CSS) to encrypt and prevent illegal copying of DVDs. However, Jon Lech Johansen, a Norwegian teenager, cracked the CSS code and posted his findings on the Internet. *See Norwegian Teen Raided by Police in DVD Suit*, Jan. 25, 2000, http://archives.cnn.com/2000/TECH/ptech/01/25/dvd.charge/index.html. Criminal charges were brought against Johansen, but he was ultimately acquitted. *See* Iain Thomson, *Norwegian Court Clears 'DVD Jon,'* Jan. 8, 2003, http://www.vnunet.com/vnunet/news/2121179/norwegian-court-clears-dvd-jon.

47. Robin D. Gross, *Digital Millennium Dark Ages*, ELECTRONIC FRONTIER FOUNDATION, Nov. 7, 2001, http://www.eff.org/IP/DMCA/Felten_v_RIAA/20011107_eff_felten_article.html; Brad King, *Real Progress in Secure Music*, WIRED NEWS, June 7, 2001, at 2, http://www.wired.com/news/mp3/0,44365-1.html?tw=wn_story_page_next1.

48. Terri Branstetter Cohen, *Anti-Circumvention: Has Technology's Child Turned Against Its Mother?*, 36 VAND. J. TRANSNAT'L L. 961, 973-74 (2003).

49. Gross, *supra* note 47.

50. *Id.*; Groennings, *supra* note 11, at 592.

sue him under the anti-circumvention provisions of the Digital Millennium Copyright Act, which prohibits "circumvent[ing] a technological measure that effectively controls access to a work protected under" the copyright statute.[51]

No lawsuit was ever brought against Professor Felten; instead, Professor Felten sued for a declaratory judgment that publication of his paper would not violate the Digital Millennium Copyright Act.[52] In response to the lawsuit, the RIAA and SDMI assured Professor Felten that they would not bring a lawsuit against him.[53] Ultimately, the case was dismissed for lack of subject matter jurisdiction, and Professor Felten subsequently published and presented his paper without any further resistance from the RIAA or SDMI.[54] Needless to say, the recording industry decided against distributing CDs with the watermarking technology.

In 2001, record labels began releasing CDs that included copy-protection technology intended to prevent consumers from listening to the CD on a computer and/or copying its contents onto the computer's hard drive.[55] Specifically, these CDs included a decoy data track on the outer edge of the CD.[56] Because of the way hard drives are programmed, a computer will continuously attempt to read this data track first before moving on to the audio tracks.[57] Thus, these copy-protected CDs could be played on standard CD players, but not on computers, certain portable devices, DVD players, and even some car stereos.[58]

The problems created by these copy-protected CDs resulted in more negative publicity for the record companies. Many consumers returned the CDs and demanded replacements without the anti-copying technology.[59] Others chose to fix it themselves—and all they needed was a magic marker or some tape.

---

51. 17 U.S.C.A. § 1201(a); Gross, *supra* note 47; Andrea L. Foster, *Princeton Cryptographer's Challenge to Music Industry Draws Computer Scientists' Support*, THE CHRONICLE OF HIGHER EDUCATION, Aug. 16, 2001, http://chronicle.com/free/2001/08/2001081602t.htm; Letter from Matthew J. Oppenheim, Esq., Senior Vice President, Recording Industry Association of America, to Professor Edward Felton [sic], Princeton University (Apr. 9, 2001), *available at* http://www.eff.org/IP/DMCA/Felten_v_RIAA/20010409_riaa_sdmi_letter.html.

52. Gross, *supra* note 47.

53. Foster, *supra* note 51.

54. Gross, *supra* note 47; Transcript of Final Hearing at 48, *Felten v. RIAA*, No. 01 CV 2669, (D. N.J. 2001), *available at* http://www.eff.org/IP/DMCA/Felten_v_RIAA/20011128_hearing_transcript.pdf.

55. *See Simple Crack Revealed for CD Copy Protection*, MEDIALINE, May 22, 2002, http://www.medialinenews.com/issues/2002/may/news0522_7.shtml.

56. *Id.*

57. *Sony's 'Copy-Proof' CD Fails to Silence Hackers*, *supra* note 41.

58. *Id.*; *CD Crack: Magic Marker Indeed*, WIRED NEWS, May 20, 2002, http://www.wired.com/news/technology/0,1282,52665,00.html; Healey & Leeds, *supra* note 41, at 2.

59. John Borland, *Customers Put Kibosh on Anti-Copy CD*, CNET NEWS, (Nov. 19, 2001), http://news.com.com/2100-1023-276036.html; *Universal to Protect U.S. Album Release*, REUTERS, Nov. 28, 2001, http://news.com.com/2100-1023-276341.html.

> When the additional track is hidden from the computer's laser by ink from a marker, a piece of electrical tape, or a piece of a self-stick memo, the computer does not attempt to read the additional track and moves on to the tracks that store the actual content, as if the CD were an ordinary audio disc.[60]

News of this "easy fix" quickly spread on the Internet, once again embarrassing the music companies that had invested significant time and resources developing this technology.[61]

## II. THE STORY OF THE SONY ROOTKIT

### A. *Sony's Copy Protection Technology*[62]

#### 1. MediaMax[63]

Despite the previous failed attempts, the recording industry did not give up on finding a marketable and secure anti-copying technology. To that end, the record labels, including Sony, sent their engineers back to the drawing board to try to find a solution to the threat posed by CD burning.[64] As a result, in the fall of 2003, Sony began releasing CDs with a new anti-copying technology called "MediaMax."[65]

Sony released CDs with two versions of the MediaMax software, 3.0 and 5.0, both of which were developed by SunnComm Technologies ("SunnComm").[66] MediaMax was like the previous generation of copy-prevention DRM in that it was intended to prevent consumers from using personal computers for unauthorized CD burning.[67] Unlike earlier DRM, however, MediaMax did not completely prohibit playing CDs on a com-

---

60. Cohen, *supra* note 48, at 995 n.7.

61. *See CD Crack: Magic Marker Indeed*, *supra* note 58.

62. *See generally* J. Alex Halderman & Edward W. Felten, *Lessons from the Sony CD DRM Episode* (Feb. 14, 2006), http://itpolicy.princeton.edu/pub/sonydrm-ext.pdf (providing a more detailed technical analysis).

63. There are two versions of the MediaMax software: 3.0 and 5.0. Settlement Agreement ¶ I.A-B, In re Sony BMG CD Techs. Litig., No. 1:05-cv-09575-NRB (S.D.N.Y. 2005), *available at* http://www.sonybmgcdtechsettlement.com/pdfs/SettlementAgreement.pdf [hereinafter Settlement Agreement]. For the most part, these versions are the same and will be discussed together. Where necessary, this article will distinguish between the two versions.

64. *See* Healey & Leeds, *supra* note 41, at 2.

65. Settlement Agreement, *supra* note 63, ¶ I.A-B; J. Alex Halderman, *Analysis of the MediaMax CD3 Copy-Prevention System*, (Oct. 6, 2003), http://www.cs.princeton.edu/~jhalderm/cd3/. Sony distributed a total of 37 titles with the MediaMax 3.0 software and 27 titles with the 5.0 version, including albums by popular artists such as the Dave Matthews Band, the Foo Fighters, Dido, Alicia Keys, and Sarah McLachlan. *See* Settlement Agreement, *supra* note 63, Ex. A.

66. Settlement Agreement, *supra* note 63, ¶ I.A-B. SunnComm is "a leader in digital content security and enhancement for optical media." Press Release, SunnComm International, SunnComm's MediaMax CD-3 Technology Passes International Test With "Flying Colors," (Aug. 27, 2003), *available at* http://www.sunncomm.com/press/pressrelease.asp?prid=20030827630 [hereinafter SunnComm Press Release].

67. *See* Halderman, *supra* note 65.

puter, but instead, limited the number of copies a user could make.[68] Specifically, it permitted users to do the following: (i) copy tracks onto the user's hard drive that could be played back without the original CD; (ii) burn tracks onto a blank CD up to three times; (iii) download tracks to certain portable devices;[69] and (iv) email tracks to friends who could listen to them for ten days.[70]

While the purpose and goal of the MediaMax DRM appear fair, the methods used to implement it, arguably, were not. When a CD containing the MediaMax program was inserted in a computer, an End User License Agreement (EULA) automatically appeared on the screen.[71] The EULA stated:

> As soon as you have agreed to be bound by the terms and conditions of the EULA, this CD will automatically install a small proprietary software program (the "SOFTWARE") onto your computer. The SOFTWARE is intended to protect the audio files embodied on the CD, and it may also facilitate your use of the DIGITAL CONTENT. Once installed, the SOFTWARE will reside on YOUR COMPUTER until removed or deleted . . . . [T]he SOFTWARE will not be used at any time to collect any personal information from you, whether stored on your computer or otherwise.[72]

---

68. Consolidated Amended Class Action Complaint ¶ 24, *In re* Sony BMG CD Techs. Litig., No. 1:05-cv-09575-NRB (S.D.N.Y. 2005), *available at* http://www.sonybmgcdtechsettlement.com/pdfs/ConsolidatedAmendedComplaint.pdf [hereinafter Sony Complaint].

69. CDs containing the MediaMax software are only compatible with Sony and Microsoft products and software, so those are the only portable devices that the tracks can be loaded onto. *Id.*

70. Halderman, *supra* note 65; Mike Snider, *Anti-Swap CD Hits the Racks*, U.S.A. TODAY, Sept. 22, 2003, at 6D, *available at* http://www.usatoday.com/tech/news/techinnovations/2003-09-22-copycd_x.htm. The MediaMax EULA describes the function of the DRM as follows:

> This CD contains technology that is designed to prevent users from making certain, unauthorized uses of the DIGITAL CONTENT, including, without limitation, the following: (1) making and storing more than one (1) copy of the DIGITAL CONTENT in each available file format on the hard drive of YOUR COMPUTER; (2) accessing the DIGITAL CONTENT on YOUR COMPUTER (once you have installed a copy of it on the hard drive of YOUR COMPUTER) using a media player that is not an APPROVED MEDIA PLAYER; (3) transferring copies of the DIGITAL CONTENT that reside on the hard drive of YOUR COMPUTER on to portable devices that are not APPROVED PORTABLE DEVICES; (4) burning more than three (3) copies of the DIGITAL CONTENT stored on YOUR COMPUTER (ATRAC OpenMG file format only) onto AtracCDs; (5) burning more than three (3) copies of the DIGITAL CONTENT onto recordable compact discs in the so-called "Red Book"-compliant audio file format; and (6) burning more than three (3) backup copies of this CD (using the burning application provided on the CD) onto recordable CDs and burning or otherwise making additional copies from the resulting backup copies.

Melcon v. Sony BMG Music Entm't, No. C 05 5084 MHP (N.D. Cal. Dec. 8, 2005), Ex. A at 2-3, *available at* http://www.eff.org/IP/DRM/Sony-BMG/ND_cal_complaint.pdf [hereinafter Melcon Complaint].

71. Settlement Agreement, *supra* note 63, ¶ I.G. The copy-prevention software only installs if the Windows "Autorun" feature is enabled, which it generally is because that is the default setting. Halderman & Felten, *supra* note 62, at 5.

72. Melcon Complaint, *supra* note 70, ¶ 21 & Ex. A.

In fact, however, the MediaMax software files (which consisted of more than a dozen files at approximately 15 MB) are loaded onto the computer *before* the user is given the opportunity to accept the EULA.[73]

MediaMax employs a temporary protection measure in order to prevent the user from copying music when the EULA is being displayed (*i.e.*, when the CD is first inserted in the computer).[74] This "temporary" protection measure installs and activates the anti-copying software before the EULA is even presented to the user.[75] The software, therefore, is installed without obtaining the user's consent.

Even worse, if the user rejects the EULA, the MediaMax software remains on the hard drive.[76] Although rejecting the EULA is supposed to deactivate the software, that is not always the case.[77] In certain situations, the software remains permanently active.[78] For example, if the 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.[79] 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.[80]

The MediaMax software also loads a type of device driver onto the computer's hard drive to prevent copying.[81] With respect to the 3.0 version, "[t]he driver examines each CD placed in the machine, and when it recognizes the protected title, it actively interferes with read operations on the audio content."[82] Similarly, the 5.0 version causes a "kernel-level driver" to be installed on the computer, the purpose of which is "to block CD ripping and copying applications from reading the audio tracks on MediaMax CDs."[83]

In addition to the obvious problems with the manner in which it was installed, the MediaMax software caused other concerns, namely, that it exchanged information between the user's computer and Sony.[84] More specifically, the MediaMax program collects personal information, including (i) the user's IP address, (ii) the type of operating system on the user's computer, (iii) the version of Internet Explorer installed on the user's computer, and (iv) the title of the MediaMax CD that the user cur-

73. Settlement Agreement, *supra* note 63, ¶ I.G.
74. Halderman & Felten, *supra* note 62, at 7.
75. *Id.*; Settlement Agreement, *supra* note 63, ¶ I.G.
76. Halderman & Felten, *supra* note 62, at 7.
77. *See id.*
78. *Id.*
79. *Id.*
80. *Id.*
81. Halderman, *supra* note 65.
82. *Id.*
83. Melcon Complaint, *supra* note 70, ¶ 18.
84. *Id.* ¶ 25; Sony Complaint, *supra* note 68, ¶ 27.

rently has loaded on his computer.[85] In light of this evidence, the statement in the EULA that "the software will not be used at any time to collect any personal information from you, whether stored on YOUR COMPUTER or otherwise,"[86] appears inaccurate.

2. XCP

In January 2005, Sony began releasing CDs with a different DRM system known as Extended Copy Protection or XCP.[87] Various versions of XCP were designed and licensed to Sony by First 4 Internet Ltd. ("F4i"),[88] a developer of content management technology based in the United Kingdom.[89] Like MediaMax, the purpose of the XCP technology was to limit, but not preclude, the use of personal computers to copy CDs.[90] For instance, 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.[91]

Also like MediaMax, the way that XCP installed itself and operated was fraught with complications. When an XCP CD was inserted in a computer, a EULA automatically appeared on the screen.[92] Among other things, the EULA provided:

> Before you can play the audio files on YOUR COMPUTER or create and/or transfer the DIGITAL CONTENT to YOUR COMPUTER, you will need to review and agree to be bound by an end user license agreement or "EULA" . . . . [I]f you do not agree to be bound by these terms and conditions, you will not be able to utilize the audio files or the DIGITAL CONTENT on YOUR COMPUTER.[93]

---

85. Melcon Complaint, *supra* note 70, ¶ 25; Sony Complaint, *supra* note 68, ¶ 27. The MediaMax software also allegedly contains an advertising program called "Perfect Placement." SunnComm described this program in a 2005 press release:

> This unique feature centrally serves up dynamic promotional content controlled by the record label to reserved spaces located throughout MediaMax interface while a user is enjoying their CD on the computer . . . . Imagine an artist's album is coming out and the record company has the ability to announce this event to all those playing the artist's previously released album on their computer.

Melcon Complaint, *supra* note 70, ¶ 32.

86. *See* Melcon Complaint, *supra* note 70, ¶ 22 & Ex. A.

87. Sony Complaint, *supra* note 68, ¶ 23. Sony released a total of 52 albums with XCP software. Settlement Agreement, *supra* note 63, Ex. A.

88. Settlement Agreement, *supra* note 63, ¶ I.B.

89. F4i Company Page, http://www.first4internet.co.uk/company.aspx (last visited Sept. 15, 2006).

90. Sony Complaint, *supra* note 68, ¶ 24.

91. Russinovich, *supra* note 4; *Sony, Rootkits and Digital Rights Management Gone Too Far*, SYSINTERNALS BLOG (Oct. 31, 2005), http://www.sysinternals.com/blog/2005/10/sony-rootkits-and-digital-rights.html; *see also* Sony Complaint, *supra* note 68, ¶ 24. The XCP EULA explaining what the user could and could not do with the CD was exactly the same as on the MediaMax EULA. *See* Melcon Complaint, *supra* note 70, Ex. B, Art. 2-3.

92. Settlement Agreement, *supra* note 63, ¶ I.G.

93. Melcon Complaint, *supra* note 70, Ex. B at ¶ 2.

Hence, if the user wanted to play the CD on a computer, he had no choice but to accept the EULA. Once the user accepted the EULA, it would not be displayed again when another CD with XCP software was loaded onto that user's computer.[94] So the user was given just one opportunity to read the following language:

> As soon as you have agreed to be bound by the terms and conditions of the EULA, this CD will automatically install a small proprietary software program . . . onto YOUR COMPUTER. The SOFTWARE is intended to protect the audio files embodied on the CD, and it may also facilitate your use of the DIGITAL CONTENT. Once installed, the SOFTWARE will reside on YOUR COMPUTER until removed or deleted. However, the SOFTWARE will not be used at any time to collect any personal information from you, whether stored on YOUR COMPUTER or otherwise.[95]

Unlike MediaMax, XCP did not use a temporary protection measure that installed software before the EULA was accepted by the user. Instead, XCP prevented copying during the installation process by monitoring the list of applications that were running on the user's computer at the time the EULA was being displayed in order to determine if the user was running a "blacklisted" ripping and copying application.[96] If such an application was found, the EULA was replaced with a warning instructing the user to close the offending application within 30 seconds or the XCP installation would terminate and the CD would be ejected.[97]

Once installed, however, the XCP software was far more dangerous than the MediaMax program because it "contains a potentially harmful 'rootkit' which renders the user's computer more vulnerable to 'malware' promulgated by third parties, including 'viruses,' 'Trojan Horses' and 'spyware,' than the computers would have been had the XCP Software not been installed."[98] The XCP EULA says nothing about this rootkit.[99]

A rootkit is "a set of software tools frequently used by a third party (usually an intruder) after gaining access to a computer system. These tools are intended to conceal running processes, files or system data, which helps an intruder maintain access to a system without the user's

---

94. Sony Complaint, *supra* note 68, ¶ 28.
95. Melcon Complaint, *supra* note 70, Ex. B ¶ 3.
96. Halderman & Felten, *supra* note 62, § 4.2.1.
97. *Id.* The warning stated:
> The installation cannot continue because there are applications running which need to be closed. Please manually close all programs shown in the list below, or click "Close Applications Now" to do it automatically. If you do not close these down within the allowed period then the installation will terminate until you next insert the disc.

*Id.*
98. Settlement Agreement, *supra* note 63, ¶ I.E.
99. Melcon Complaint, *supra* note 70, Ex. B.

knowledge."[100] Rootkits are not visible to a computer's operating system, nor can they be detected by antivirus and security software.[101]

Here, the Sony rootkit functioned by integrating itself in the computer's operating system and then concealing all files that began with "$sys$," which included the XCP copy-prevention software.[102] The danger of this "cloaking mechanism" is that any file can be made invisible to the user by assigning it a name that begins with "$sys$."[103] Consequently, users who have played Sony CDs containing XCP software on their computers are left vulnerable to hackers.[104]

Not only did the XCP software install this rootkit, but, contrary to the EULA, it also gathered personal information from the user's computer.[105] Like the MediaMax software, the XCP program communicated the user's IP address and the title of the CD the user was currently playing to Sony.[106] Additionally, when Sony's server received the information about what CD was being played, it "automatically check[ed] for updates to the album art and lyrics for that album, . . . [which] uses the bandwidth that would otherwise be available to the user's computer for other tasks."[107] Thus, both the MediaMax and XCP systems "phone home" with personal information regarding Sony's consumers.[108]

### *B. The Discovery of Sony's Copy Protection Technology*

#### 1. Alex Halderman and the MediaMax Software

When CDs with the MediaMax copy-prevention system were released in September 2003, it was not a secret. SunnComm issued a press release lauding its new technology,[109] and numerous newspaper articles

---

100. Security Reference Guide, *The Sony Rootkit: What It Is and How to Remove It*, INFORMIT.COM, para. 4 (Sept. 15, 2006), http://www.informit.com/guides/content.asp?g=security&seqNum=192&rl=1 (citation omitted).

101. Melcon Complaint, *supra* note 70, ¶ 52.

102. Sony Complaint, *supra* note 68, ¶ 35; Melcon Complaint, *supra* note 70, ¶¶ 51-53.

103. Sony Complaint, *supra* note 68, ¶ 35.

104. *Id.* ¶ 36; Nancy Lang-Feldman, *Sony's Rootkit Is All Evil*, COMPUTER SHOPPER, ¶ 4 (Mar. 2006), http://shopper.cnet.com/4002-7409_9-6457527.html.

105. Settlement Agreement, *supra* note 63, ¶ I.E; Sony Complaint, *supra* note 68, ¶ 27.

106. Melcon Complaint, *supra* note 70, ¶¶ 59-60; Sony Complaint, *supra* note 68, ¶ 27.

107. Melcon Complaint, *supra* note 70, ¶ 59.

108. Bruce Schneier, *Real Story of the Rogue Rootkit*, WIRED NEWS, (Nov. 17, 2005), http://www.wired.com/news/privacy/0,1848,69601,00.html.

109. SunnComm Press Release, *supra* note 66, ¶¶ 2-4. The press release stated:

> MediaMax CD3 products passed all tests and met the toughest standards. . . . It achieved a very high level of playability combined with an incredible level of security for the music. . . . [T]he functionality and security level offered by the MediaMax technology was pushed to the limit. The testing results were able to verify playability on consumer electronic devices, stability of the product on computers and robustness of the security features to protect content against unauthorized copying when used with CD ripper programs [sic].

*Id.*

were written on the topic.[110] Moreover, the MediaMax CDs contained warnings. For example, the album cover stated: "This CD is protected against unauthorized duplication. It is designed to play on standard playback devices and an appropriately configured computer (see system requirements on back). If you have questions or concerns visit http://www.sunncomm.com/support/bmg."[111] And the face of the CD itself stated: "This disc is protected against unauthorized duplication."[112]

However, consumers were not warned about the manner in which the MediaMax program operated (*i.e.*, that the software files were installed even if the EULA was declined), nor were they aware the software was communicating personal information to Sony.[113] That changed in October 2003 when J. Alex Halderman, a Ph.D. student in computer science at Princeton University, published a paper analyzing the MediaMax software.[114] Not only did Halderman describe how the MediaMax software worked, he explained that a user can easily bypass the software by holding down the shift key for a few seconds while loading a CD onto the computer.[115]

Once again, the record industry's hopes for a marketable and secure copy-protection system were quickly dashed. Mr. Halderman's publica-

---

110. *U.S. Firm Hopes Anti-Piracy CD Will Rock Blackmarket*, BUS. TIMES, ¶ 1 (Sept. 26, 2003), http://web.archive.org/web/20031024232303/http:/it.asia1.com.sg/newsdaily/news006_2003 0926.html (reporting "SunnComm Technologies Inc. said on Wednesday it has designed a revolutionary CD with embedded anti-piracy technology that it hopes will rock the black-market trade in pirated music"); Frank Ahrens, *BMG Offers Legal Song Sharing*, WASH. POST, Sept. 23, 2003, at E1; Jon Healey, *BMG is Releasing Copy-Protected CDs*, LA TIMES, Sept. 13, 2003, at C3.

111. Halderman, *supra* note 65, § 2. The "systems requirements" on the back of the CD provided:

> THIS CD IS ENHANCED WITH MEDIAMAX SOFTWARE. Windows Compatible Instructions: Insert disc into CD-ROM drive. Software will automatically install. If it doesn't, click on 'LaunchCd.exe.' MacOS Instructions: Insert disc into CD-ROM drive. Click on "Start." Usage of the CD on your computer requires your acceptance of the End User License Agreement and installation of specific software contained on the CD. Windows System Requirements: Windows 98/2000/XP, Internet Explorer 5.5 or later, Windows Media Player 7.1 or compatible player. Mac System Requirements: Mac OSX 10.1, Power Mac G3/G4, iMac, eMac, Powerbook G3/G4, iBook with 128 Mb of RAM, Windows Media Player for Mac OSX, Internet Explorer 5.2, Monitor capable of displaying 800x600 screen resolution & 256 colors (64K colors recommended), 12x or faster multi-session-enabled CD-ROM drive, Flash Player 6. Digital files on this CD will also play on portable devices supporting secure WMA files. Certain computers may not be able to access the enhanced portion of this disc. None of the manufacturers, developers, or distributor make any representation or warranty, or assumes any responsibility, with respect to the enhanced portion of this disc.

*Id.*

112. *Id.*

113. Halderman & Felten, *supra* note 62, §§ 4.2.2, 6.

114. Halderman, *supra* note 65. Mr. Halderman is a student of Professor Felten's and was part of the team that removed the digital watermark in response to the SDMI challenge in 2000. *See supra* Part I.B.2; *see also* http://www.cs.princeton.edu/~jhalderm/.

115. Halderman, *supra* note 65, § 3. Halderman also reported that, only four days after the release of *Comin' From Where I'm From* by Anthony Hamilton (Arista Records/BMG), a CD containing the MediaMax DRM, he searched peer-to-peer networks and discovered that every song from that album was available to be downloaded. *Id.*

tion was particularly devastating for SunnComm, whose stock fell nearly 25% within forty-eight hours of the paper hitting the Internet.[116] SunnComm responded by threatening to sue Halderman for violation of the anti-circumvention provisions of the Digital Millennium Copyright Act.[117] Ultimately, however, SunnComm decided against filing suit against Mr. Halderman, presumably because doing so would turn an already bad situation into a complete public relations nightmare.[118]

2. Mark Russinovich and the XCP Software

In late October 2005, Mark Russinovich, a computer security analyst, discovered a hidden software program on his computer that he believed was a rootkit.[119] Mr. Russinovich was able to trace the software program to a Sony CD he had recently played on his computer.[120] Mr. Russinovich then attempted to remove the rootkit, but realized he could not do that without compromising his computer system.[121]

After further investigation, Mr. Russinovich also discovered that the XCP software "engage[ed] in 'phone home' behavior."[122] Specifically, the software connected to Sony's servers and provided the customer's IP address,[123] as well as a code associated with the CD that the customer was listening to on his computer.[124]

On October 31 and November 4, 2005, Mr. Russinovich published his findings about the Sony rootkit in great detail on his weblog.[125] News of Sony's potentially dangerous software program spread quickly on the

116. *SunnComm Says Pointing to Shift Key "Possible Felony,"* Oct. 9, 2003, *available at* http://yro.slashdot.org/article.pl?sid=03/10/09/2211259&mode=nested&tid=123&tid=126&tid=141&tid=172&tid=188&tid=93&tid=99; *SunnComm Threatens Suit Over Shift Key Circumvention*, Oct. 10, 2006, *available at* http://grep.law.harvard.edu/article.pl?sid=03/10/10/0917244; Kevin Maney, *Debate Heats Up As Student Spots Hole In CD Protection*, USA TODAY, *available at* http://www.usatoday.com/money/industries/technology/2003-10-26-princeton-cover_x.htm.

117. Tony Smith, *SunnComm to Sue "Shift Key" Student for $10 Million*, THE REGISTER, Oct. 9, 2003, *available at* http://www.theregister.co.uk/2003/10/09/sunncomm_to_sue_shift_key.

118. Declan McCullagh, *SunnComm Won't Sue Grad Student*, CNET NEWS, Oct. 10, 2005, http://news.com.com/2100-1027-5089448.html ("SunnComm's threats had drawn enormous attention in a short time, with some legal analysts saying a lawsuit would represent an egregious abuse of the DMCA."); *SunnComm Technologies Reverses Decision to Bring Legal Action Against Princeton Researcher*, Oct. 10, 2003, http://www.sunncomm.com/press/pressrelease.asp?prid=200310101150.

119. Affidavit of Mark Russinovich in Support of Plaintiffs' Motion for Final Approval of Class Action Settlement ¶ 7, at 2; *In re Sony BMG CD Tech. Litig.*, Case No. 1:05-cv-09575-NRB, ¶ 7 (S.D.N.Y. 2006) [hereinafter Russinovich Affidavit], *available at* http://www.sonybmgcdtechsettlement.com/pdfs/RussinovichAffISOFinalApp-4-5-06.pdf; *see also* Nate Mook, *Lawsuit Fights Back Against Sony DRM*, BETANEWS, Nov. 10, 2005, http://www.betanews.com/article/Lawsuit_Fights_Back_Against_Sony_DRM/1131635264 ("Russinovich first reported on the software after his company's security tool recognized a "rootkit" on his machine.").

120. Russinovich Affidavit, *supra* note 119, ¶¶ 7-8, at 2.

121. *Id.* ¶ 11; Andrew Kantor, *Sony: The Rootkit of All Evil?*, USA TODAY, Nov. 17, 2005, *available at* http://www.usatoday.com/tech/columnist/andrewkantor/2005-11-17-sony-rootkit_x.htm.

122. Russinovich Affidavit, *supra* note 119, ¶ 14, at 4-5.

123. Settlement Agreement, *supra* note 63, ¶ I.E.

124. Russinovich Affidavit, *supra* note 119, ¶ 14, at 4-5.

125. *Id.* ¶¶ 7, 14 & Exs. B & C.

Internet, and ultimately to the mainstream media.[126] On November 10, 2005, Symantec Corporation, a computer security company, announced that it had discovered the first XCP-related virus, which "tears down firewalls and gives hackers access to personal computers."[127] The public was outraged and demanded a response from Sony.[128]

### C. *Sony's Response to Discovery of the Rootkit*

Sony's initial response to Mr. Russinovich's discovery was to deny any wrongdoing and defend its software.[129] During an interview on National Public Radio, Thomas Hesse, President of Sony's Global Digital Business, said: "Most people I think don't even know what a rootkit is, so why should they care about it?"[130] Mr. Hesse further indicated that the software was only included on about twenty titles, when in fact, the number was closer to fifty.[131] He also admitted that the software was cloaked "so would-be pirates can't find it and remove it."[132] Finally, Mr. Hesse said that "no information ever gets gathered about the user's behavior. No information ever gets communicated back. . . . This is purely about restricting the ability to burn MP3 files in an unprotected manner."[133]

After further media exposure and numerous customer complaints, Sony released a program that was supposed to remove the XCP "cloaking mechanism," as well as uninstall tools for both the MediaMax and

---

126. Sony Complaint, *supra* note 68, ¶ 34; Mook, *supra* note 119.

127. Sony Complaint, *supra* note 68, ¶ 38; Gregg Keizer, *Sony Issues Patch As Hackers Pounce on Rootkit*, INFORMATIONWEEK, Nov. 3, 2005, http://informationweek.comn/shared/printableArticleSrc.jhtml?articleID=173402819.

128. *See* Nate Mook, *Sony to Help Remove Its DRM Rootkit*, BETANEWS, Nov. 2, 2005, http://www.betanews.com/article/Sony_to_Help_Remove_its_DRM_Rootkit/1130965475. The comments to this news story demonstrate the outrage felt by many members of the public. *Id.* Some swore off purchasing CDs, others vowed never to buy another Sony product, and some viewed Sony's conduct as an excuse to download music illegally. As one person explained, "This is now a reason for me to only download music illegally. They are shooting their own feet off with this crap." *Id.*

129. Interview with Thomas Hesse, National Public Radio, Nov. 4, 2005, *available at* http://www.npr.org/templates/story/story.php?storyId=4989260 [hereinafter NPR Interview]. There is evidence that Sony learned about the rootkit and the potential problems it could cause about a month before Mr. Russinovich published his findings on the Internet. *See* Steve Hamm, *Sony BMG's Costly Silence*, BUS. WEEK, Nov. 29, 2005, http://www.businessweek.com/technology/content/nov2005/tc20051129_938966.htm. John Guarino, owner of a small PC repair shop in New York, had been removing a mysterious rootkit from his clients' hard drives for months. *Id.* He investigated the problem using a rootkit detector software manufactured by a Finnish company called F-Secure. *Id.* Using that software, he was able to confirm on September 30, 2005, that the rootkit was caused by Sony copy-protected CDs. *Id.* Mr. Guarino notified F-Secure who conducted its own investigation. *Id.* On October 4, F-Secure told Sony about the rootkit, and Sony, in turn, asked F4i to investigate. Within approximately two weeks, F-Secure provided a full report to Sony regarding the rootkit, and described XCP as a "major security risk." *Id.* Nevertheless, it was Mark Russinovich, not Sony, who informed the public about the rootkit problem on October 31, 2005. *Id.*

130. NPR Interview, *supra* note 129.

131. *See* Settlement Agreement, *supra* note 63, Ex. A.

132. NPR Interview, *supra* note 129.

133. *Id.*

XCP copy-prevention software.[134] However, as Mr. Russinovich and others discovered, these software patches actually created additional risks to users' computers.[135] Consequently, on or about November 15, 2005, Sony announced that it would recall all CDs containing the XCP software and would instate a consumer exchange program for those who had already bought the copy-protected CDs.[136] There was no similar recall or exchange program with respect to MediaMax CDs.

### *D. Sony Rootkit Litigation*

#### 1. Consumer Class Action Suits

On November 1, 2005, the day after Mr. Russinovich published his findings about the rootkit on the Internet, the first of many class action lawsuits was filed against Sony and the manufacturers of the MediaMax and XCP software.[137] These lawsuits alleged that Sony's "manufacture, sale and distribution of DRM-enhanced music CDs, especially in the absence of appropriate warnings and disclosure," [138] violated the Computer Fraud and Abuse Act, 18 U.S.C. § 1030, the consumer fraud, false advertising, and/or deceptive trade practices laws of several states, and state and federal common law.[139] Because several of these lawsuits were

---

134. Russinovich Affidavit, *supra* note 119, ¶¶ 16-17; Sony Complaint, *supra* note 68 ¶¶ 39-40. However, Sony made it difficult to obtain the XCP uninstall tool. Russinovich Affidavit, *supra* note 119, ¶¶ 17-18.

135. Russinovich Affidavit, *supra* note 119, ¶ 16; Sony Complaint, *supra* note 68, ¶¶ 47-49; Electronic Frontier Foundation, EFF Does Not Recommend Patch at This Time (Dec. 6, 2005) *available at* http://www.eff.org/news/archives/2005_12.php; *see also* Halderman & Felten, *supra* note 63, at 22-23.

136. Tom Sanders, *Sony Backs Out of Rootkit Anti-Piracy Scheme*, VNUNET.COM, Nov. 15, 2005, http://www.vnunet.com/vnunet/news/2146053/sony-backs-root-kit-anti-piracy; Russinovich Affidavit, *supra* note 119, ¶ 20. As of late November, however, CDs containing XCP software were still available in stores. *See* Arik Hesseldahl, *Spitzer Gets on Sony BMG's Case, New York Attorney General has turned his attention to Sony BMG's copyright fiasco*, BUSINESS WEEK ONLINE, Nov. 29, 2005, http://businessweek.com/technology/content/nov2005/tc20051128_573560.htm.

> On November 29, 2005 the New York Attorney General Elliot Spitzer found through his investigators that despite the recall of November 15 Sony BMG CDs with XCP were still for sale in New York City music retail outlets. Spitzer said 'It is unacceptable that more than three weeks after this serious vulnerability was revealed, these same CDs are still on shelves, during the busiest shopping days of the year,' 'I strongly urge all retailers to heed the warnings issued about these products, pull them from distribution immediately, and ship them back to Sony.' On November 30, 2005, Massachusetts Attorney General Tom Reilly issued a statement saying that Sony BMG CDs with XCP were still available in Boston despite the Sony BMG recall of November 15. Attorney General Reilly advised consumers not to purchase the Sony BMG CDs with XCP and said that he was conducting an investigation of Sony BMG.

Wikipedia, *Sony CD Copy Protection Controversy*, http://en.wikipedia.org/wiki/2005_Sony_CD_copy_protection_controversy; *see also* Hesseldahl, *supra* note 136.

137. Settlement Agreement, *supra* note 63, ¶¶ I.C., I.D. (listing lawsuits filed to date against Sony).

138. Memorandum of Law in Support of Plaintiffs' Motion for Final Approval of Class Action Settlement at 6, *In re: Sony BMG CD Techs. Litig.*, Case No. 1:05-cv-09575 (NRB) (S.D.N.Y. 2006), *available at* http://www.sonybmgcdtechsettlement.com/pdfs/MEMOOFLAWISOFINAL APPROVAL4-6-06.pdf [hereinafter Final App. Motion].

139. *Id.*; Settlement Agreement, *supra* note 63, ¶ I.I. Many of the lawsuits that were filed in California also asserted California's Consumer Protection Against Computer Spyware Act, Cal. Bus.

filed in the United States District Court for the Southern District of New York, on December 1, 2005, those actions were consolidated and lead counsel was appointed (hereinafter "Consolidated Action").[140]

In late December, the parties in the Consolidated Action reached a settlement. On December 28, 2005, the Settlement Agreement was filed with the court in conjunction with the parties' request for preliminary approval of the settlement.[141] In exchange for a release of all claims related to the MediaMax or XCP software, defendants agreed, among other things, to:

(i) Recall all XCP CDs;

(ii) Maintain an ongoing exchange program so customers could receive the CD they purchased without the copy-protection software;

(iii) Distribute a free, effective uninstall tool for both the MediaMax and XCP software programs;

(iv) Provide cash awards and free music downloads to class members;

(v) Agree not to use DRM software to collect personal information;[142]

(vi) Improve disclosures on future copy-protected CDs; and

(vii) Have an independent third party test any future copy-protection software for security risks.[143]

The settlement benefits for customers affected by the XCP software are clearly better than for those customers who purchased MediaMax CDs. For example, XCP customers can elect to receive cash where MediaMax customers are limited to free downloaded music.[144] Moreover, Sony did not agree to recall MediaMax CDs as it did with XCP CDs. The apparent reason for this is because plaintiffs believe that "MediaMax, while harmful, does not pose the same level of danger to end users and their computer systems as XCP, because MediaMax does not contain

---

& Prof. Code § 22947-22947.6. *See, e.g.*, Melcon Complaint, *supra* note 70, ¶ 160 (N.D. Cal. Dec. 8, 2005).

140. Final App. Motion, *supra* note 138, at 7.

141. Settlement Agreement, *supra* note 63, at 1; *see also* FED. R. CIV. P. 23(e)(1)(A) ("The court must approve any settlement, voluntary dismissal, or compromise of the claims, issues, or defenses of a certified class.").

142. However, "Personal Data" as defined in the Settlement Agreement "does *not* include the IP address of the computer's Internet connection or any information with respect to an album title, artists and tracks, or other non-personally identifiable information, that is routinely logged by SONY BMG in connection with enhanced or connected CDs." Settlement Agreement, *supra* note 63, ¶ II.H (emphasis added). *Cf. infra* Part III.B.2. (arguing that such data does constitute personally identifiable information).

143. Settlement Agreement, *supra* note 63, ¶¶ III.B-C, K, M, S, IV.B.3.f, h; Final App. Motion, *supra* note 138, at 9-10. Sony recently settled class action suits in Canada on terms substantially identical to those in the U.S. settlement. *See Sony BMG Settles Canadian 'Rootkit' Cases; Tex. Suit Continues*, CONSUMER ELECTRONICS DAILY, Sept. 1, 2006, *available at* 2006 WLNR 15459519 [hereinafter *Sony BMG Settles Candian 'Rootkit' Cases*].

144. Settlement Agreement, *supra* note 63, ¶¶ III.C, E-F.

a rootkit that installs hidden files on an end user's system and evades detection from firewalls, anti-spyware and anti-virus software."[145]

On January 6, 2006, the Court conditionally certified the class and granted preliminary approval.[146] As of April 6, 2006, only two objections had been filed.[147] On May 22, 2006, the court held a fairness hearing, and subsequently granted final approval of the settlement.[148] Class members have until the end of 2006 to file claims,[149] so it is unclear at this point what the total cost of this settlement will be for defendants.

2. Government Inquiries

The rootkit incident not only caught the attention of the plaintiffs' class action bar, it spurred numerous government inquires as well. Since December 2005, Sony has been the subject of an inquiry by the Federal Trade Commission and has been investigated by numerous state attorney generals and other governmental authorities throughout the United States.[150] Indeed, Stewart Baker, the assistant secretary for policy in the Department of Homeland Security, directed the following comments at Sony in response to the rootkit incident: "It is very important to remember that it's your intellectual property—it's not your computer. And in pursuit of protection of intellectual property, it's important not to defeat or undermine the security measures that people need to adopt in these days."[151]

To date, however, only one law enforcement action has actually been filed against Sony. On November 21, 2005, the Texas Attorney General, Greg Abbott, sued Sony under that state's Consumer Protection against Computer Spyware Act of 2005, Tex. Bus. & Com. Code § 48.001 *et seq.*[152] This is the first suit that has ever been brought under the recently enacted spyware law.[153] The Texas action, which concerns

145. Russinovich Affidavit, *supra* note 119, ¶ 23.

146. Final App. Motion, *supra* note 138, at 10.

147. *Id.* at 18.

148. Anne Broache, *Sony Rootkit Settlement Gets Final Nod*, CNET NEWS, May 22, 2006, http://news.com.com/Sony+rootkit+settlement+gets+final+nod/2100-1030_3-6075370.html; *see also* FED. R. CIV. P. 23(e)(C) ("The court may approve a settlement, voluntary dismissal, or compromise that would bind class members only after a hearing and on finding that the settlement, voluntary dismissal, or compromise is fair, reasonable and adequate.").

149. Welcome to the Information Web Site for the Sony BMG CD Technologies Settlement, http://www.sonybmgcdtechsettlement.com/ImportantDates.htm (last visited September 2, 2006) [hereinafter Welcome to the Information Website].

150. Settlement Agreement, *supra* note 63, ¶ I.M; *see, e.g.*, Kurt Opsahl, *Florida AG's Office Enters Sony BMG DRM Fray*, DEEP LINKS NOTEWORTHY NEWS FROM AROUND THE INTERNET, Jan. 3, 2006, http://www.eff.org/deeplinks/archives/004292.php; *Sony BMG Settles Canadian 'Rootkit' Cases*, *supra* note 143.

151. Russinovich Affidavit, *supra* note 119, ¶ 19.

152. Plaintiff's Original Petition, ¶¶ 14-16, State of Texas v. Sony BMG Music Entm't, LLC, No. GV505065 (126th Tex. Dist. Ct. Nov. 21, 2005), *available at* http://www.oag.state.tx.us/newspubs/releases/2005/112105sony_pop.pdf [hereinafter Texas Petition]; *Texas Sues Sony BMG for Spyware*, COMPUTER & INTERNET LAWYER, Feb. 2006, at 31.

153. *Texas Sues Sony BMG for Spyware*, *supra* note 152, at 31.

only the XCP software, makes claims similar to those asserted in the consumer class action lawsuits discussed in the previous section.[154]

Sony is currently in negotiations with Attorney General Abbott and other law enforcement agents to try to settle these matters. In fact, the Settlement Agreement in the Consolidated Action provides that: "The Parties expect that, by the date of the Fairness Hearing, SONY BMG will have entered into an enforceable, nationwide agreement resolving one or more of the Government Inquiries."[155] But the fairness hearing has come and gone and yet no settlement has been reached and the Texas action continues to proceed.[156]

Sony has been able to resolve the litigation resulting from the rootkit debacle rather quickly. But this is not the end of the story. The rootkit debacle has disillusioned consumers, lawmakers, and artists alike. Moreover, it has raised numerous legal questions that are sure to arise the next time Sony or another record label releases copy-protected CDs.

## III. LEGAL QUESTIONS RAISED BY THE SONY ROOTKIT DEBACLE

The Sony rootkit debacle has raised numerous legal issues, and this section focuses on those at the heart of the controversy surrounding the recording industry's use of digital rights management (DRM) to protect its intellectual property. First, it analyzes Sony's potential liability for manufacturing and distributing CDs containing MediaMax and XCP software, including (i) whether it violated the Computer Fraud and Abuse Act and the Texas Consumer Spyware Act of 2005,[157] and (ii) whether Sony's copy-prevention software comported with copyright law, specifically the fair use doctrine. Second, this section examines the Digital Millennium Copyright Act of 1998, which prohibits the circumvention of DRM technology, and the potential legal exposure created by that statute for Sony customers and security researchers.

---

154. *Compare* Texas Petition, *supra* note 152, ¶¶ 7-13 *and* Sony Complaint, *supra* note 68, ¶¶ 1-4.

155. Settlement Agreement, *supra* note 63, ¶ IV.A.

156. Welcome to the Information Website, *supra* note 149; *Sony BMG Settles Candian 'Rootkit' Cases*, *supra* note 143.

157. There are numerous state law claims that were or potentially could have been asserted against Sony, such as trespass to chattels, unfair business practices, and fraud. *See* Sony Complaint, *supra* note 68, ¶¶ 68-99 (alleging non-disclosure, deceptive acts and practices, false advertising, breach of implied covenant of good faith and fair dealing, trespass to chattels, common law fraud, and negligent misrepresentation); Melcon Complaint, *supra* note 70, ¶¶ 90-114 (alleging material misrepresentations and omissions of fact, unconscionability and unreasonableness, and computer contamination in violation of California Penal Code § 502). Because evaluating every potential cause of action against Sony is beyond the scope of this article, it focuses on the Computer Fraud and Abuse Act, the only federal statute asserted against Sony, and the Texas Consumer Spyware Act, the only law that a government agency has alleged was violated by Sony's conduct. Texas Petition, *supra* note 152, ¶¶ 14-16; Sony Complaint, *supra* note 68, ¶¶ 58-67.

*A. Sony's Potential Liability*[158]

1. Computer Fraud and Abuse Act

The Computer Fraud and Abuse Act (CFAA), which was enacted in 1984, was the first comprehensive federal computer crime statute.[159] The CFAA outlaws seven types of conduct: (1) knowingly accessing a computer without authorization, or exceeding authorized access, to obtain national security information;[160] (2) intentionally accessing a computer without authorization, or exceeding authorized access, to obtain information;[161] (3) intentionally accessing without authorization a computer used by the federal government;[162] (4) knowingly accessing a "protected computer" without authorization, or exceeding authorized access, with intent to defraud;[163] (5) intentionally accessing a "protected computer" without authorization and causing damage;[164] (6) knowing fraudulent trafficking of computer passwords;[165] and (7) transmitting communications that threaten to damage a "protected computer" with intent to extort.[166]

The CFAA is a criminal statute that also provides for a civil cause of action.[167] Pursuant to section 1030(g), a civil lawsuit can be brought if (i) plaintiff suffered damage or loss due to a violation of the statute, and (ii) the conduct at issue involved one of the five factors listed in 18 U.S.C. § 1030(a)(5)(B).[168] The first factor—"loss to 1 or more persons during any 1-year period (and, for purposes of an investigation, prosecution, or other proceeding brought by the United States only, loss resulting from a related course of conduct affecting 1 or more other protected computers) aggregating at least $5,000 in value"—is the one that litigants generally rely upon.[169]

---

158. Sony likely would argue it was unaware of how the copy-prevention software operated, and therefore, should not be held liable for any damage it may have caused. This article presumes that Sony's attempt to make such an argument would fail.

159. 18 U.S.C.A. § 1030 (West 2006); Dodd S. Griffith, *The Computer Fraud and Abuse Act of 1986: A Measured Response to a Growing Problem*, 43 VAND. L. REV. 453, 474-82 (1990).

160. § 1030(a)(1).

161. § 1030(a)(2).

162. § 1030(a)(3).

163. § 1030(a)(4).

164. § 1030(a)(5).

165. § 1030(a)(6).

166. § 1030(a)(7).

167. § 1030(g).

168. Southwest Airlines v. Farechase, Inc., 318 F. Supp. 2d 435, 439 (E.D. Tex. 2004) ("A careful reading of the statute shows that a civil plaintiff is not required to state a cause of action pursuant to subsection (a)(5), but merely to allege one of the factors enunciated in subsection (a)(5)(B).").

169. § 1030(a)(5)(B)(i). The other four factors are:

> (ii) the modification or impairment, or potential modification or impairment, of the medical examination, diagnosis, treatment, or care of 1 or more individuals; (iii) physical injury to any person; (iv) a threat to public health or safety; or (v) damage affecting a computer system used by or for a government entity in furtherance of the administration of justice, national defense, or national security.

*Id.* § 1030(a)(5)(B)(ii)-(v).

a. Is there a cause of action under § 1030(a)(5)(B)?

In the Consolidated Action, plaintiffs asserted that Sony violated section 1030(a)(5)(B) of the CFAA by intentionally accessing customers' computers without authorization and, as a result of such conduct, causing damage—namely the "loss to 1 or more persons during any 1-year period . . . aggregating at least $5,000 in value."[170] To prevail on this claim, plaintiffs would have been faced with two potential stumbling blocks: the $5,000 damage provision and the unauthorized access requirement.[171]

i. CFAA's $5,000 Damage Provision

Under section 1030(a)(B)(5) of the CFAA, plaintiffs must prove "damage" or "loss" of at least $5,000.[172] This is often an insurmountable barrier to the individual computer user because "[e]ven the most expensive personal computer costs much less than this."[173] Moreover, it is not clear what type of damage or loss is sufficient to meet the CFAA's $5,000 requirement. Some courts have held that the damage or loss must be related to investigating or remedying damage to a computer.[174] Others have concluded that damage to reputation or goodwill counts toward the damage threshold.[175] "The question this raises for the individual con-

170. Sony Complaint, *supra* note 68, ¶¶ 59-67.

171. The statute also provides that the defendant access a "protected computer," which is limited to computers used by a financial institutions, the United States Government, or in interstate commerce or communication. *See* § 1030(e)(2). In the past, this requirement posed an additional hurdle because most computers were not used in these capacities. *See, e.g.*, Benjamin J. Patterson, *Spyware Covertly Infringing on Your Internet Privacy While Circumventing the Federal Legislation Radar*, 54 DRAKE L. REV. 233, 249-50 (2005). However, if a computer is connected to the Internet, it more than likely is used in interstate commerce or communication. Although a significant number of Americans still do not use the Internet, most of those people do not have a computer. *See* Jim Downing, *Americans Who Use the Internet*, SMART MOBS, Oct. 6, 2005, *available at* http://www.smartmobs.com/archive/2005/10/06/americans_who_u.html; *Nearly 150 Million Adult Americans Use the Internet, Survey Says*, FOX.COM, Apr. 28, 2006, *available at* http://www.foxnews.com/story/0,2933,193417,00.html. Thus, while there may be some computers that are not connected to the Internet and, therefore, would not meet the "protected computer" requirement, they are a small minority. Downing, *supra* note 171; § 1030(e)(2). This is particularly true with respect to those individuals harmed by the Sony rootkit, because the vast majority of people who listen to music on their computers are also Internet users.

172. Whether a plaintiff claims "damages" or "losses" under the CFAA, courts have held that plaintiff is subject to the $5,000 threshold. *See In re* DoubleClick Inc. Privacy Litig., 154 F. Supp. 2d 497, 522 (S.D.N.Y. 2001).

173. Alan F. Blakley et al., *Coddling Spies: Why the Law Doesn't Adequately Address Computer Spyware*, 2005 DUKE L. & TECH. REV. 25, 33.

174. *See, e.g.*, Nexans Wires S.A.. v. SARK-USA, Inc., 319 F. Supp. 2d 468, 473-74 (S.D.N.Y. 2004) (stating that costs unrelated to computer repair, such as travel costs for business that could have been conducted by telephone, do not constitute "loss" within the meaning of the CFAA); ResDev, LLC v. Lot Builders Ass'n, 6:04_cv_1374_Orl_31DAB, 2005 U.S. Dist. LEXIS 19099, at *9-12 (M.D. Fla. 2005) ("The CFAA's 'loss' definition . . . list[s] costs that are similar in that they are all directly associated with, or with addressing, an unauthorized-computer-access event.").

175. America Online, Inc. v. LCGM, 46 F. Supp. 2d 444, 451 (E.D. Va. 1998).

sumer is whether litigation and the necessity of experts to show the extent of loss are worth the chance of recovery."[176]

Even where, as here, a class action has arisen, the damage provision can still pose a problem because courts are divided on whether plaintiffs' claims can be aggregated to meet the $5,000 minimum.[177] In *Thurmond v. Compaq Computer Corporation,*[178] the court held that aggregation is not permitted under the CFAA because the statute requires damage to "*a* protected computer," *i.e.*, a *single* computer.[179] The court explained that "no one can bring a cause of action unless the defendant causes an aggregate of $5,000 'damage' to a protected computer. If defendant causes such damage, then any injured person may bring a claim even if, his or her own 'damage,' is less than $5,000."[180]

In *In re DoubleClick Inc. Privacy Litigation,*[181] the court analyzed the CFAA's legislative history and held that plaintiffs could only aggregate damages and losses across victims and time for a *single act* by the defendant.[182] In reaching this conclusion the court relied on the fact that "damage" is defined as "any impairment to the integrity or availability of data, *a* program, *a* system, or information."[183] That Congress used the singular form of these words rather than the plural (*i.e.*, programs, systems) indicates that the statute should apply only to single acts.[184]

By contrast, in *In re: America Online, Inc. (AOL),*[185] the court held that the $5,000 threshold applies to all computers that the defendant's unlawful conduct affected.[186] The court specifically considered, and rejected, the decisions in *Thurmond* and *DoubleClick* on the grounds that they were not binding precedent, they misread the statute, and they misinterpreted the legislative history.[187] The court further explained that interpreting the CFAA as *Thurmond* and *DoubleClick* courts did,

> would lead to the absurd result that a party who accesses one computer without authorization, and thereby causes $5,000 worth of damage to that one computer, would be guilty of violating the CFAA and, therefore, civilly liable. On the other hand, a party who accesses

176. Blakley et al., *supra* note 173, at 33.
177. Luke J. Albrecht, *Online Marketing: The Use of Cookies & Remedies for Internet Users*, 36 SUFFOLK U. L. REV. 421, 431-33 (2003).
178. 171 F. Supp. 2d 667, 681 (E.D. Tex. 2001).
179. § 1030(a)(5)(A)(iii) (emphasis added).
180. *Thurmond*, 171 F. Supp. 2d at 681.
181. 154 F. Supp. 2d 497 (S.D.N.Y. 2001).
182. *Double Click*, 154 F. Supp. 2d at 523-24.
183. § 1030(e)(8) (emphasis added).
184. *DoubleClick*, 154 F. Supp. 2d at 523.
185. 168 F. Supp. 2d 1359 (S.D. Fla. 2001).
186. *In re* America Online, Inc., 168 F. Supp. 2d 1359, 1374 (S.D. Fla. 2001).
187. The *AOL* court also distinguished these cases on another ground: "Moreover, their precedent did not allow them to aggregate damages until the classes had been certified. In the Eleventh Circuit, the rule is opposite, for a case is treated as a class action until certification is denied." *Id.* at 1373.

> millions of computers and causes only $100 worth of damage to each computer would not be guilty of violating the CFAA.[188]

In light of this split among district courts, it is unclear to what extent plaintiffs may aggregate their damages in alleging a CFAA violation. Nevertheless, in a lawsuit against Sony for damage caused by its copy-protection software, plaintiffs would be able to satisfy the $5,000 minimum regardless of whether the court applied the *Thurmond*, *DoubleClick*, or *AOL* rule.

Under *Thurmond*, as long as plaintiffs can demonstrate that at least one class member suffered $5,000 in "damage" or "loss" the threshold is met.[189] This includes "any reasonable cost to any victim, including the cost of responding to an offense, conducting a damage assessment, and restoring the data, program, system, or information to its condition prior to the offense . . . ."[190] Given the extreme difficulty customers experienced trying to remove (or have someone else remove) the software from their computer systems, it is highly likely that at least one individual suffered $5,000 in damages.[191]

Plaintiffs also would have been able to demonstrate a "single act" as required by the court in *DoubleClick*.[192] As alleged in the complaint: "SONY BMG's act of producing its master encoded tapes through which DRM CDs were made, was a single act that proximately resulted in damages greater than $5,000."[193] At the very least, even if the production of MediaMax CDs was separate from the production of XCP CDs, each of these acts alone caused more than $5,000 in damage to Sony customers.[194] Thus, plaintiffs would have satisfied the *DoubleClick* test.

Finally, there is no doubt that plaintiffs easily would have met the $5,000 damage threshold under *AOL*, which allows the aggregation of all damage caused by defendants to any victim.[195] Sony manufactured more than 20 million CDs with MediaMax software, and more than 5 million with XCP software.[196] These CDs were installed on tens of thousands of

---

188. *Id.* at 1374.
189. *Thurmond*, 171 F. Supp. 2d at 681.
190. § 1030(e)(11).
191. Russinovich Affidavit, *supra* note 119, ¶ 11. Section 1030(e)(11) also provides for the recovery of consequential damages, including, but not limited to, lost revenue. § 1030(e)(11). However, section 1030(g) – the provision that grants plaintiffs the right to bring a civil action – says that "[d]amages for a violation involving only conduct described in subsection (a)(5)(B)(i) are limited to *economic damages*." *Id.* § 1030(g) (emphasis added). Courts have interpreted this provision to mean that "compensatory damages for such conduct will be awarded only for economic harm." P.C. Yonkers, Inc. v. Celebrations the Party & Seasonal Superstore, LLC, 428 F.3d 504, 511 (3d Cir. 2005).
192. *DoubleClick*, 154 F. Supp. 2d at 523.
193. Sony Complaint, *supra* note 68, ¶ 66.
194. *See id.*
195. *In re AOL*, 168 F. Supp. 2d at 1373-74.
196. Sony Complaint, *supra* note 68, ¶¶ 33, 44.

computers throughout the United States, and damages far exceeded the $5,000 minimum.[197]

ii. CFAA's Unauthorized Access Provision

Section 1030(a)(5)(B) additionally requires plaintiffs to demonstrate that defendant accessed a computer without authority.[198] More specifically, the subsection of the CFAA asserted against Sony provides that "[w]hoever . . . intentionally accesses a protected computer *without authorization*, and as a result of such conduct, causes damage; and . . . by [such] conduct . . . caused . . . loss to 1 or more persons during any 1-year period . . . aggregating at least $5,000 in value . . . shall be punished . . . ."[199] In other words, the applicability of the CFAA depends on whether the owner of the CD consented to the installation of the MediaMax and/or XCP software on his computer.[200]

In cases like this one involving the installation of software, the question of consent generally turns on the End User License Agreement (EULA). A EULA is an agreement "between a producer and a user of computer software, which grants the user a software license."[201] The EULA is usually presented to the user electronically, and installation of the software is conditioned upon the user accepting the EULA.[202] These types of agreements are often referred to as "shrinkwrap licenses."[203]

The use of EULAs in connection with computer software has been the subject of great debate. Because EULAs are lengthy, contain overly restrictive, non-negotiable terms, and frequently are not read by users, many commentators have criticized the use of these agreements.[204] In *Specht v. Netscape Communications Corporation*,[205] the Second Circuit held that a EULA was unenforceable because "a consumer's clicking on

197. *See id.* ¶¶ 60, 66.

198. § 1030(a)(5)(B).

199. § 1030(a)(5) (emphasis added). Plaintiffs also asserted claims under § 1030(a)(5)(A)(i) ("[w]hoever . . . knowingly causes the transmission of a program, information, code, or command, and as a result of such conduct, intentionally causes damage without authorization, to a protected computer") and § 1030(a)(5)(A)(ii) ("[w]hoever . . . intentionally accesses a protected computer without authorization, and as a result of such conduct, recklessly causes damage"). Sony Complaint, *supra* note 68, ¶ 59(b), (c). For present purposes, however, it is only necessary to analyze subsection (iii) since that burden is the lowest for plaintiffs to overcome.

200. *See* Wayne R. Barnes, *Rethinking Spyware: Questioning the Propriety of Contractual Consent to Online Surveillance*, 39 U.C. DAVIS L. REV. 1545, 1565 (2006) ("[T]he fact that the CFAA only penalized 'unauthorized' computer access presupposes that any consent or authorization which has been given to the accessing entity will create a defense to liability under the CFAA.").

201. Wikipedia, *Software License Agreement* (2006), http://en.wikipedia.org/wiki/software_license_agreement.

202. *Id.*

203. F. Lawrence Street & Mark P. Grant, *The Law of the Internet*, § 103[1] (Brian Elias et al. eds., Matthew Bender & Co., Inc., Release No. 9 2005) (1997).

204. *See* Michael L. Rustad & Thomas H. Koenig, *The Tort of Negligent Enablement of Cybercrime*, 20 BERKELEY TECH. L.J. 1553, 1562-63 (2005); *see also* Batya Goodman, Note, *Honey, I Shrink-Wrapped the Consumer: The Shrink-Wrap Agreement as an Adhesion Contract*, 21 CARDOZO L. REV. 319 (1999); Barnes, *supra* note 200, at 1547.

205. 306 F.3d 17 (2d Cir. 2002).

a download button does not communicate assent to contractual terms if the offer did not make clear to the consumer that clicking on the download button would signify assent to those terms."[206]

By contrast, other courts have upheld these agreements regardless of how unfair they may seem. In *i.Lan Systems, Inc. v. Netscout Service Level Corporation*,[207] for example, the court held that clicking on the "I Agree" box was sufficient consent to form a contract.[208] Similarly, in *ProCD, Inc. v. Zeidenberg*,[209] the Seventh Circuit held that shrinkwrap licenses are enforceable because, in many common transactions, contracts are considered valid even though the consumer purchases the product before being presented with the detailed terms of the contract.[210]

Here, the question whether acceptance of Sony's EULA provides the necessary "consent" or "authorization" under the CFAA depends not only on the terms of the EULA, but also on the manner in which the anti-copying software was installed and how it operated. Although the terms of the MediaMax and XCP EULA were essentially identical, as described above, there were differences in the installation and operation of the two software programs. Accordingly, MediaMax and XCP must be analyzed separately under the CFAA.

a.) MediaMax Was Installed "Without Authorization"

MediaMax attempted to protect the content on the CD from being ripped and copied while the EULA was being displayed by immediately installing, and at least temporarily activating, the anti-copying software.[211] In other words, the MediaMax software was installed before the user accepted the EULA and, thus, "without authorization."[212] Even if the user ultimately rejected the EULA, the software remained on his computer, and, in some cases, remained permanently active.[213]

The facts of this case are far more egregious than in *Specht v. Netscape*[214] where the court determined there was no informed consent be-

206. *Specht*, 306 F.3d at 29-30; *see also* Step-Saver Data Sys., Inc. v. Wyse Tech., 939 F.2d 91, 98 (3d Cir. 1991); SoftMan Prods. Co. v. Adobe Sys., Inc., 171 F. Supp. 2d 1075, 1088 (C.D. Cal. 2001); Arizona Retail Sys., Inc. v. Software Link, Inc., 831 F. Supp. 759, 765 (D. Ariz. 1993); Klocek v. Gateway, Inc., 104 F. Supp. 2d 1332, 1341 (D. Kan. 2000); U.S. Surgical Corp. v. Orris, Inc., 5 F. Supp. 2d 1201, 1206 (D. Kan. 1998).

207. 183 F. Supp. 2d 328 (D. Mass 2002).

208. *i.Lan*, 183 F. Supp. 2d at 338; *see also* M.A. Mortenson Co. v. Timberline Software Co., 998 P.2d 305, 311-14 (Wash. 2000); Caspi v. Microsoft Network, L.L.C., 732 A.2d 528, 532 (N.J. Super. Ct. App. Div. 1999).

209. 86 F.3d 1447 (7th Cir. 1996).

210. *ProCD*, 83 F.3d at 1452; *see also* Lexmark Int'l Inc. v. Static Control Components, Inc., 387 F.3d 522, 563 n.10 (6th Cir. 2004); Hill v. Gateway 2000, Inc., 105 F.3d 1147, 1149-50 (7th Cir. 1997); Meridian Project Sys., Inc. v. Hardin Construction Co., 426 F. Supp. 2d 1101, 1107 (E.D. Cal. 2006).

211. Settlement Agreement, *supra* note 63, ¶ I.G.; Halderman & Felten, *supra* note 62, at 7.

212. Settlement Agreement, *supra* note 63, ¶ I.G.; Halderman & Felten, *supra* note 62, at 7.

213. Halderman & Felten, *supra* note 62, at 7.

214. *Specht*, 306 F.3d at 21-25.

cause the EULA did not make clear that clicking on the download button constituted acceptance of the contract.[215] Here, the user did not even have a chance to view the EULA, much less accept it, before the software was installed.[216] Thus, this case is similar to *Register.com, Inc. v. Verio, Inc.*[217] and *Softman Products Co. v. Adobe Systems, Inc.*[218]

In *Register.com*, the plaintiff was a registrar of domain names, meaning it issued domain names to persons and entities preparing to establish web sites on the Internet.[219] In applying for a domain name applicants were required to submit certain information to Register.com ("Register"), including name, address, telephone number, and email address.[220] This identifying information was referred to as "WHOIS information."[221]

The Internet Corporation for Assigned Names and Numbers (ICANN), a private non-profit corporation established by U.S. government agencies to administer domain names, requires companies like Register to update the WHOIS information daily and to make such information publicly available.[222] An entity submitting a "WHOIS query" to Register would receive the requested information together with the following message: "By submitting a WHOIS query, you agree that you will use this data only for lawful purposes and that under no circumstances will you use this data to support the transmission of mass unsolicited, commercial advertising or solicitation via email."[223]

The defendant, Verio, Inc. ("Verio"), sells web site design, development, and operation services.[224] In order to attract customers, Verio obtained daily updates from the WHOIS information, and then sent those individuals marketing information by email, telemarketing, and direct mail.[225] As noted above, the terms and conditions that were included in Register's query responses prohibited the use of WHOIS information to solicit by email.[226] Accordingly, Register sued Verio for violation of the CFAA and trespass to chattels.[227]

In defense Verio argued that it was not bound by Register's terms and conditions "because, in the case of each query Verio made, the [terms and conditions] did not appear until after Verio had submitted the

215. *Id.* at 29-30.
216. Settlement Agreement, *supra* note 63, ¶ I.G.
217. 356 F.3d 393 (2d Cir. 2004).
218. 171 F. Supp. 2d 1075 (C.D. Cal. 2001).
219. *Register.com*, 356 F.3d at 395.
220. *Id.*
221. *Id.*
222. *Id.*
223. *Id.* at 397.
224. *Id.* at 396.
225. *Id.* at 396-97.
226. *Id.*
227. *Id.* at 397.

query and received the WHOIS data."[228] In other words, Verio contended it never received legally enforceable notice of Register's terms and conditions.[229] Although the court ultimately rejected this argument, before doing so it explained: "If Verio had submitted only one query, or even if it had submitted only a few sporadic queries, that would give considerable force to its contention that it obtained the WHOIS data without being conscious that Register intended to impose conditions, and without being deemed to have accepted Register's conditions."[230] Along those same lines, the dissenting judge concluded:

> By the time Register.com presents its proposed terms, it has already given away that which it "owns" – access to its WHOIS database . . . . Thus, in the single submission scenario, an end-user would have had no opportunity to reject Register.com's terms and would be bound to comply with them irrespective of actual assent . . . . [T]he submission of a WHOIS query prior to the presentation of Register.com's proposed terms [is] insufficient to constitute a manifestation of assent.[231]

*Register.com*, therefore, stands for the proposition that a party cannot assent to a contract before having the opportunity to review the terms and conditions of that contract.[232]

Similarly, in *Softman Products Co. v. Adobe Systems, Inc.*,[233] Adobe Systems Inc. ("Adobe"), a developer and publisher of software, sued SoftMan Products Co. ("SoftMan"), a company that distributed computer software programs through its website www.buycheapsoftware.com, claiming that SoftMan was infringing Abode's copyright and trademark as well as violating terms of its license by distributing Adobe's software in an unauthorized manner.[234] There was no direct contractual relationship between Adobe and SoftMan, instead, Adobe claimed that SoftMan's distribution of the software violated the EULA that end-users are asked to assent to when they attempt to install Adobe software.[235]

Among other things, SoftMan contended that it was not bound by the terms of the EULA because it never assented to that agreement.[236] The court agreed with SoftMan, holding that

> there is only assent on the part of the consumer, if at all, when the consumer loads the Adobe program and begins the installation process. It is undisputed that SoftMan has never attempted to load the

228. *Id.* at 401.
229. *Id.*
230. *Id.*
231. *Id.* at 431 (Parker, J., dissenting).
232. *Id.* at 430-31 & n.43 (Parker, J., dissenting).
233. *SoftMan*, 171 F. Supp. 2d 1075.
234. *Id.* at 1079-80.
235. *Id.* at 1080.
236. *Id.* at 1087.

> software that it sells. Consequently, the Court finds that SoftMan is not subject to the Adobe EULA.[237]

The holdings of *Register.com* and *SoftMan* make clear that Sony had no right to install the MediaMax software before the end-user even had an opportunity to view the EULA's terms and conditions. As such, Sony accessed its customers' computers without authority in violation of 18 U.S.C. § 1030(a)(5)(B).

b.) XCP Was Not Installed "Without Authorization"

The XCP software used a different tool to prevent ripping and copying during the installation process. As described in greater detail above, it searched for "blacklisted" ripping and copying applications, and precluded users who were running such applications from downloading the software and listening to the music on the CD. Consequently, the XCP software was not installed onto a user's computer until the EULA was accepted.

Nor did the XCP EULA suffer from the defects identified in *Specht v. Netscape*.[238] The XCP EULA stated:

> This End-User License Agreement ("EULA") is a legal agreement between you and SONY BMG MUSIC ENTERTAINMENT ("SONY BMG"), a general partnership established under Delaware law. By clicking on the "AGREE" button below, you will indicate your acceptance of these terms and conditions, at which point this EULA will become a legally binding agreement between you and SONY BMG.[239]

Because the EULA made clear that the user was assenting to the terms the rationale of *Netscape* does not apply.

Moreover, while it is true that the XCP EULAs did not fully disclose the nature of the software being installed,[240] that alone is not enough to prove that Sony accessed the computers "without authorization." The decision in *In re: America Online*[241] is instructive on this point.[242] There, computer users sued AOL under section 1030(a)(5) of the CFAA (the same provision asserted against Sony) claiming that AOL 5.0, a software program that had been recently released, damaged computers and prohibited utilization of competitors' software.[243] AOL moved to dismiss this claim on the grounds that its access was not "with-

---

237. *Id.*
238. *Specht*, 306 F.3d at 29-30.
239. Sony Complaint, *supra* note 68, ¶ 28.
240. *See supra* Part II.A. (discussing the details of the MediaMax and XCP EULAs and software features).
241. *In re AOL*, 168 F. Supp. 2d 1359.
242. *Id.* at 1359.
243. *Id.* at 1363-64.

out authorization" since "the consumers expressly authorized installation of AOL 5.0 on their computers."[244] At most, AOL argued "it exceeded the scope of its authority by distributing defective software, but exceeding the scope of authorization is not a situation that is covered by 18 U.S.C. § 1030(a)(5), the only provision under which the consumers have brought suit."[245]

After examining the plain language of the statute, the court agreed with AOL.[246] Section 1030(a)(5) requires that the access be "without authorization"; it says nothing about the access "exceeding authorization."[247] By contrast, several provisions of the CFAA – namely, sections 1030(a)(1),[248] (2),[249] and (4),[250] – specifically state that a violation occurs if defendant accesses a computer without authorization *or* if it exceeds authorized access.[251] The CFAA further provides that "exceeds authorized access" means "to access a computer with authorization and to use such access to obtain or alter information in the computer that the accessor is not entitled to so obtain or alter."[252] Hence, the *AOL* court decided Congress clearly intended to distinguish between "without authorization" and "exceeds authorized access."[253]

If Congress wanted section 1030(a)(5) to apply to defendants who exceed authorized access it would have included that term within the scope of section 1030(a)(5) as it did with the other subsections of 1030(a). "[W]here Congress includes particular language in one section of a statute but omits it in another section of the same Act, it is generally presumed that Congress acts intentionally and purposely in the disparate inclusion or exclusion."[254] Thus, even though Sony and/or F4i may have "exceeded authorized access" by installing XCP software on customers' computers, the plain language of the statute and the cases interpreting it would likely preclude plaintiffs from recovering under section 1030(a)(5) of the CFAA.[255]

---

244. *Id.* at 1368.
245. *Id.* at 1368-69.
246. *Id.* at 1369-70.
247. § 1030(a)(5).
248. § 1030(a)(1) ("having knowingly accessed a computer without authorization or *exceeding authorized access* . . . .") (emphasis added).
249. § 1030(a)(2) ("intentionally access a computer without authorization *or exceeds authorized access* . . . .") (emphasis added).
250. § 1030(a)(4) ("knowingly and with intent to defraud, accesses a protected computer without authorization, or *exceeds authorized access* . . . .") (emphasis added).
251. § 1030(a)(1), (a)(2), (a)(4).
252. § 1030(e)(6).
253. *In re AOL*, 168 F. Supp. 2d at 1369-70.
254. Gozlon-Peretz v. United States, 498 U.S. 395, 404 (1991) (quoting Russello v. United States 464 U.S. 16 (1983)).
255. *See* Int'l Airport Ctrs., L.L.C. v. Citrin, 440 F.3d 418, 420 (7th Cir. 2006) ("The difference between 'without authorization' and 'exceeding authorized access' is paper thin, but not quite invisible." (citations omitted)).

b. Is there a cause of action under other provisions of the CFAA?

Although the CFAA claims asserted against Sony in the Consolidated Action relied solely upon section 1030(a)(5)(B), Sony may also have violated other provisions of the CFAA. Subsection 1030(a)(2)(C), for example, prohibits intentionally accessing a computer without authorization, or exceeding authorized access, to obtain "information from any protected computer if the conduct involved an interstate or foreign communication."[256]

The MediaMax and XCP EULA stated that "the SOFTWARE will not be used at any time to collect any personal information from you, whether stored on YOUR COMPUTER or otherwise."[257] Yet, in truth, both MediaMax and XCP contained "phone home" capabilities, meaning these software programs gathered information from users' computers, including IP addresses and the title of the CD being played on the user's computer, and communicated that information back to Sony.[258] Under these circumstances, even if customers accepted the EULA, they clearly did not consent to Sony's use of the software to collect personal information. Accordingly, Sony was accessing its customers' computers without authorization or, at the very least, exceeding authorized access.

Subsection 1030(a)(2)(C) also requires the "conduct," *i.e.*, the act of "accessing a computer," to involve an interstate or foreign communication.[259] Here, Sony accessed its customers' computers with software that was included on CDs, which are products sold in interstate commerce, and then used that software to communicate information from the customer's computer back to Sony and/or the software manufacturer.[260] Such conduct plainly involves interstate communications, and, therefore, this requirement is satisfied. Hence, a cause of action should lie pursuant to section 1030(a)(2)(C).

Nevertheless, a question remains as to who can bring a lawsuit under section 1030(a)(2)(C) of the CFAA. While the government undoubtedly could bring a criminal action under this provision of the CFAA, it is not as clear whether a civil claim could be asserted as well. Section 1030(g) of the CFAA provides for a civil lawsuit where (i) the plaintiff suffered damage or loss due to a violation of the statute, and (ii) the con-

256. § 1030(a)(2)(C).
257. Sony EULA, http://www.sysinternals.com/blog/sony-eula.htm (last visited Sept. 7, 2006).
258. Sony Complaint, *supra* note 68, ¶ 27.
259. § 1030(a)(2)(C). *See* C.H. Robinson Worldwide, Inc. v. Command Transp., LLC, No. 05 C 3401, 2005 WL 3077998, at *4 (N.D. Ill. Nov. 16, 2005); Charles Schwab & Co. v. Carter, No. 04 C 7071, 2005 WL 2369815, at *8 (N.D. Ill. Sept. 27, 2005).
260. Sony Complaint, *supra* note 68, ¶¶ 30, 64.

duct at issue involved one of the five factors listed in 18 U.S.C. § 1030(a)(5)(B).[261]

Many litigants, including plaintiffs in the Consolidated Action, apparently interpret this language to mean that a civil action under the CFAA can only be brought under section 1030(a)(5)(B).[262] And, in fact, at least one court has come to the same conclusion.[263] In recent years, however, several courts have considered the issue and now the weight of authority leans heavily in the other direction.

In *P.C. Yonkers v. Celebrations the Party & Seasonal Superstore*,[264] for example, the court held that a civil action could be stated under any provision of the CFAA as long as the plaintiff alleges one of the five factors enumerated in subsection (a)(5)(B), which includes a loss in excess of $5,000.[265] Moreover, in *I.M.S. Inquiry Management Systems, Ltd. v. Berkshire Information Systems, Inc.*,[266] the defendant argued that plaintiff could not state a claim under section 1030(a)(2)(C) on the grounds that section 1030(g) does not provide a civil cause of action for violations of this subsection.[267] The court rejected this argument, finding that:

> The plain text of § 1030(g) does not provide or imply, and defendant offers no supporting case law for, such a restriction. Section 1030(g) affords a civil action for any CFAA violation, but requires an allegation of one of five enumerated factors in § 1030(a)(5)(B). Plaintiff's Amended Complaint satisfies § 1030(g) by elsewhere alleging the consequence described in § 1030(a)(5)(B)(i) (loss aggregating to at least $5,000).[268]

Like the defendant in *I.M.S.*,[269] (i) Sony exceeded authority in accessing its customers' computers, (ii) it obtained information from its customers by such conduct, (iii) that conduct involved interstate communications, and (iv) as a result of such conduct, Sony caused at least $5,000 in loss or damage to its customers. Consequently, Sony, too, would be subject to civil suit under section 1030(a)(2)(C) of the CFAA for its conduct with respect to both the MediaMax and XCP software.

---

261. § 1030(g).

262. Sony Complaint, *supra* note 68, ¶¶ 59, 62.

263. McLean v. Mortgage One & Fin. Corp., No. 04-1158, 2004 U.S. Dist. LEXIS 7279, at *5 (D. Minn. Apr. 9, 2004) (holding that section 1030(g)'s reference to subsection (a)(5)(B) limits civil relief to claims under subsection (a)(5)(B)).

264. 428 F.3d 504 (3d Cir. 2005).

265. *Yonkers*, 428 F.3d at 512.

266. 307 F. Supp. 2d 521 (S.D.N.Y. 2004).

267. *I.M.S.*, 307 F. Supp. 2d at 525-26.

268. *Id.* at 526.

269. Other courts similarly have determined that a civil cause of action lies under § 1030(a)(2)(C). *See, e.g.*, Theofel v. Farey-Jones, 341 F.3d 978, 986 (9th Cir. 2003); Chance v. Avenue A, Inc., 165 F. Supp. 2d 1153, 1158 (W.D. Wash. 2001); *In re* Intuit Privacy Litig., 138 F. Supp. 2d 1272, 1279-80 (C.D. Cal. 2001).

2. Texas Spyware Act

Spyware is software that is covertly installed onto a computer, for example by bundling it with other software that the user downloads.[270] Once installed, spyware transmits information from the user's computer to the servers of the entity responsible for installing the spyware.[271] "Spyware can monitor everything users do with their machines, not only their activities on the web, and transmit that information to an outside entity."[272] The use of spyware has grown dramatically in recent years. In fact, one study shows that more than 80% of personal computers in the United States are infected by spyware, although most users are unaware of it.[273]

Consequently, federal and state legislators have been working to enact laws to address this very serious threat. In 2005, the U.S. House of Representatives passed two spyware-related bills: (1) the Securely Protect Yourself Against Cyber Trespass Act,[274] and (2) the Internet Spyware (I-Spy) Prevention Act of 2005.[275] The Senate also is considering a spyware bill called the Spy Block Act,[276] which was approved by the Senate Commerce Committee in 2005, but was not voted on by the full Senate.[277] To date, however, no further action has been taken by Congress on any of these bills. According to one commentator, Congress may be revising the bills "in view of issues raised late in 2005 by Sony's Rootkit copy-protection software and the associated end-user-license-agreement."[278]

In the absence of federal legislation, some states, including Texas, have taken it upon themselves to outlaw spyware.[279] The Texas Consumer Protection Against Computer Spyware Act ("Texas Spyware Act"), Tex. Bus. & Com. Code § 48.001 et seq., came into effect on September 1, 2005.[280] Generally, the statute prohibits the following conduct: (1) unauthorized collection or culling of personally identifiable informa-

---

270. Laurel L. Poe, Comment, *The SPY Act: A Bandage for an Ever-Festering Sore or an Efficient Safeguard for the American Consumer?*, 22 T.M. COOLEY L. REV. 329, 331 (2005).

271. *Id.* at 335.

272. Blakley, *supra* note 173, at 28. *See also* Erica Pines, Note, *Spyware Regulation: National Legislation Should Prompt Industry Self-Policing*, 38 LOY. L.A. L. REV. 2219, 2219 (2005) ("Spyware can change individual computer settings, track personal information numbers, store credit card numbers, and access all personal data stored on a computer's hard drive, thereby shredding away every bit of privacy personal computer users think they have.").

273. Poe, *supra* note 270, at 329-30.

274. H.R. 29, 109th Cong. § 1 (2005).

275. H.R. 744, 109th Cong. § 1 (2005).

276. S. 687, 109th Cong. § 1(a) (2005).

277. Britt L. Anderson, *Is Anti-Spyware Legislation Congress's Killer App in 2006?*, 4 No. 2 INTERNET L. & STRATEGY 1, 4 (Feb. 2006).

278. *Id.*

279. Michael L. Baroni, *Spyware Beware*, 47 ORANGE COUNTY LAWYER 36, 38 (Apr. 2005) (stating that Utah and California have also enacted spyware-related laws).

280. TEX. BUS. & COM. CODE ANN. § 48.001 (West 2006).

tion;[281] (2) unauthorized access to or modifications of computer settings;[282] (3) unauthorized interference with installation or disabling of computer software;[283] (4) inducement of computer user to install unnecessary software;[284] and (5) copying and execution of software to a computer with deceptive intent.[285] The Texas Spyware Act also provides for a civil right of action, which applies to users of personal and business computers, and permits private parties to obtain damages of $100,000 for each violation.[286]

On November 21, 2005, the Texas Attorney General sued Sony for violation of the Texas Spyware Act – the first lawsuit under the new statute.[287] Specifically, Texas asserts that, by marketing, distributing, and selling CDs with XCP software, Sony has violated section 48.053 of the Texas Spyware Act.[288] That section, which concerns the unauthorized interference with installation or disabling of computer software, provides:

> If a person is not the owner or operator of the computer, the person may not knowingly cause computer software to be copied to a computer in this state and use the software to:
>
> (1) prevent, through intentionally deceptive means, reasonable efforts of the owner or operator of the computer to block the installation or execution of or to disable computer software by causing computer software that the owner or operator has properly removed or disabled to automatically reinstall or reactivate on the computer;
>
> (2) intentionally misrepresent to another that computer software will be uninstalled or disabled by the actions of the owner or operator of the computer;
>
> (3) remove, disable, or render inoperative, through intentionally deceptive means, security, antispyware, or antivirus computer software installed on the computer;
>
> (4) prevent the owner's or operator's reasonable efforts to block the installation of or to disable computer software by:

281. § 48.051.
282. § 48.052.
283. § 48.053.
284. § 48.055(1).
285. § 48.055(2).
286. § 48.101(a), (b)(2)(B).
287. Texas Petition, *supra* note 152, ¶ 2; *Texas Sues Sony BMG for Spyware*, *supra* note 152, at 31; News Release, Attorney General Abbott Brings First Enforcement Action in Nation Against Sony BMG for Spyware Violations (Nov. 21, 2005), *available at* http://www.oag.state.tx.us/oagNews/release.php?id=1266.
288. Texas Petition, *supra* note 152, ¶¶ 14-16. Unlike the civil lawsuits discussed above, this case involves XCP only, not MediaMax. Texas Petition, *supra* note 152, ¶ 7.

> (A) presenting the owner or operator with an option to decline the installation of software knowing that, when the option is selected, the installation process will continue to proceed; or
>
> (B) misrepresenting that software has been disabled;
>
> (5) change the name, location, or other designation of computer software to prevent the owner from locating and removing the software; or
>
> (6) 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.[289]

Of particular importance to the case against Sony are the last two clauses. Subsection (5) prohibits a person from changing the name or location of software to prevent the computer user from finding and removing the software.[290] Similarly, subsection (6) prohibits the creation of randomized or deceptive file names or folders to prevent removal of the software.[291] As discussed above, this is exactly what the rootkit installed by the XCP did: it concealed all files that began with "$sys$," including the copy-prevention software, so that the files could not be located and removed. Indeed, Thomas Hesse, President of Sony's Global Digital Business, admitted this during his NPR interview when he explained that the software was cloaked "so would be pirates can't find it and remove it."[292] It thus appears, based on the plain language of the statute, that Sony violated the Texas Spyware Law.[293]

3. Does Sony's Copy-Prevention Software Violate Copyright Law?

Most people were outraged by the Sony rootkit incident because the software created security risks to and collected information from the user's computer, *not* because Sony was limiting the number of copies of the CD the customer could make. Allegations that Sony was using spyware and causing serious damage to customers' computers overshadowed the question whether Sony's copy-protection software impinged on customers' rights under copyright law, in particular the fair use doctrine. However, this is an important question to examine given Sony and the

289. TEX. BUS. & COM. CODE ANN. § 48.053 (West 2006).
290. § 48.053(5).
291. § 48.053(6).
292. NPR Interview, *supra* note 129.
293. It is important to note, however, that the Texas Spyware Act has never been "tested" in the courts, and therefore, Sony could assert certain defenses to invalidate the statute. In particular, Sony may argue that the Texas Spyware Act is unconstitutional because it violates the dormant commerce clause, which limits states' authority to enact laws that unduly burden interstate commerce. *Cf.* Pines, *supra* note 272, at 2230-39 (analyzing California's spyware act and concluding that it violates the dormant commerce clause).

other record labels are certain to continue to use DRM technology to copy-protect CDs.[294]

a. Fair Use Doctrine

Copyright law grants copyright owners the exclusive right to copy and distribute copyrighted works.[295] "Fair use" is an exception to this exclusive right that allows copying for certain limited purposes, including commenting on, criticizing, reporting about, or parodying a copyrighted work.[296] It is the fair use doctrine, for example, that allows a book critic to quote from the novel she is reviewing without obtaining permission from the copyright owner.[297] Thus, fair use protects the public interest in a free exchange of ideas and discourse.[298]

Fair use is a deliberately imprecise and flexible doctrine. It "permits [and requires] courts to avoid rigid application of the copyright statute when, on occasion, it would stifle the very creativity which that law is designed to foster."[299] There are no bright line rules for deciding whether certain conduct constitutes fair use.[300] Instead, courts make that decision on a case-by-case basis by considering at least the following four factors:

> (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;

---

294. Settlement Agreement, *supra* note 63, ¶ IV.B (setting forth guidelines that Sony must follow in the future when developing DRM technology). As an RIAA Spokesperson recently explained:

> DRM and copy protection are important parts of the creative process, serving to protect the work of musicians and labels and promote responsible personal use by fans. They are no silver bullet, nor were they ever intended to be. They are one component of a larger effort to protect our works from theft . . . . DRM is a key piece of the digital future, not just for music companies but also for movie studios, software companies and countless other intellectual property industries.)

*Digital Rights Management (DRM): Media Companies' Next Flop?*, Jan. 26, 2006, http://forum.ecoustics.com/bbs/messages/34579/192800.html; Richard Gooch, *Setting the Record Straight on DRM*, Feb. 3, 2006, http://www.ifpi.org/site-content/press/20060203.html ("DRM is the key to our successful digital music business. It enables consumers to get exactly what they pay for, and to pay for exactly for what they get. But to work in the future DRM will need support from our technology partners and from governments.").

295. 17 U.S.C.A. § 106(1), (3) (West 2006).

296. 17 U.S.C.A. § 107.

297. *See id.*

298. *See* Campbell v. Acuff-Rose Music, Inc., 510 U.S. 569, 575 (1994) (stating that the fair use doctrine is necessary "to fulfill copyright's very purpose, 'to promote the Progress of Science and useful Arts'").

299. *Campbell*, 510 U.S. at 577 (alteration in original) (quoting Stewart v. Abend, 495 U.S. 207, 236 (1990)).

300. *Id.*

> and (4) the effect of the use upon the potential market for or value of the copyrighted work.[301]

Because fair use has been left ambiguous so it can evolve over time, the doctrine is often misunderstood. By way of example, many people believe that "personal" or non-commercial use (*e.g.*, copying lawfully acquired copyrighted materials for one's personal use) is always fair use.[302] This is not true.[303] While courts have found that the fair use doctrine protects certain personal uses of copyrighted materials, there is no blanket statutory or common law rule protecting this behavior.[304]

The most well-known case addressing the question whether personal use falls within the fair use exception is *Sony Corporation of America v. Universal City Studios, Inc.* [305] In that case, Universal and other copyright owners sued Sony for copyright infringement based on its manufacture of the video cassette recorder ("VCR"), a novel product at the time.[306] Plaintiffs argued that Sony should be held liable because it knew or should have known that its customers would engage in infring-

---

301. 17 U.S.C.A. § 107.

302. *See* Fair Use, Wikipedia: The Free Encyclopedia, http://en.wikipedia.org/wiki/Fair_use (last modified Sep. 1, 2006) (discussing the doctrine of fair use in the United States). *See also* The Big Picture, DRM Crippled CD: A Bizarre Tale in 4 Parts, Oct. 31, 2005, http://bigpicture.typepad.com/comments/2005/10/drm_crippled_cd.html. As one music fan explained their understanding of fair use:

> I am a buyer of CDs, and only rarelydo [sic] I download tracks from Apple's iTunes Music Store due to *sound quality*. I didn't spend an obscene amount of money on a home audio system to listen to the mediocre audio quality of MP3s. The not-even-remotely-as-lossless-as-advertised-compression algorithms are hardly any better. MP3s and iPod quality music is fine for the beach or my commute on a train, but its something else entirely in my living room. *My fair use*: When I get a new CD, I rip it to iTunes, then transfer the music to my iPods; I make a backup copy (in case of loss). If I really like a disc, I make a copy for the car or the weekend house. If the disc is 'youth-friendly,' I'll make a copy for my wife's classroom. She teaches art, and I refuse to let her take any more original discs to school—they have all gotten destroyed. Incidentally, I am what the marketing people like to call an *'influencer'* (i.e., think of Netflix, TiVo or Macintosh). I do not copy entire CDs for people, but I like to expose friends to news [sic] music—I will give them a song or two, with the recommendation that if they like it, they purchase the artist's disc. I use P2P to check out stuff not available elsewhere, or to see if I want to purchase a full CD. I also like to make mixed playlists, which get burned for the car or for friends who are looking to hear new music, now that radio is dead. I believe all of the above is well within my rights as a consumer of the CDs that I legally purchased; If someone wants to try to convince me otherwise, please take your best shot.

*Id.*

Even worse, some people apparently believe that it is fair use to let your friends make pirated copies of CD's. *See id.* ("[P]irating the album is the [sic] now the sole *best* way to get this album, because you can get a 100% compatible, full quality copy that you can't even buy in the store.").

303. *See* JOINT REPLY COMMENTS OF AAP: ASSOCIATION OF AMERICAN PUBLISHERS, ET AL., EXEMPTION TO PROHIBITION ON CIRCUMVENTION OF COPYRIGHT PROTECTION SYSTEMS FOR ACCESS CONTROL TECHNOLOGIES, at 39 (2006) [hereinafter JOINT REPLY], *available at* http://www.copyright.gov/1201/2006/reply/11metalitz_AAP.pdf.

304. *See id.* at 31-33, 39.

305. 464 U.S. 417 (1984).

306. *Sony Corp.*, 464 U.S. at 420.

ing activity, *i.e.*, the taping of copyrighted television programs and films.[307]

At trial, however, the evidence demonstrated that Sony's customers used their VCRs primarily to "time-shift," *i.e.*, to tape a program so that it could be viewed at a later, more convenient time, which the Court determined was a non-infringing fair use.[308] The evidence further showed that Sony did not manufacture the VCR explicitly to encourage or cause its customers to tape copyrighted programs, nor did Sony take active steps to increase its profits from illegal taping.[309] Thus, there was no basis to hold Sony liable for inducement of infringement, and the only theory available to plaintiffs was contributory infringement.[310] The Court went on to hold that, because the VCR is "capable of commercially significant noninfringing use" (*i.e.*, time-shifting programs), Sony could not be held liable for infringement based solely on distribution of the product.[311]

Another important case regarding "personal use" of copyrighted materials is *Recording Industry Association of America v. Diamond Multimedia Systems, Inc.*[312] There, the Recording Industry Association of America (RIAA) sought a preliminary injunction against the manufacturer of the Rio, a portable MP3 player, on the grounds that the Rio did not meet the requirements for digital audio recording devices under the Audio Home Recording Act of 1992 (AHRA).[313] AHRA "prohibits legal actions for copyright infringement based on the manufacture, importation, or distribution of digital audio equipment or media for private, noncommercial recording."[314] AHRA also prohibits infringement actions against the consumers of these products as long as they are being used for a noncommercial purpose.[315]

In return, AHRA requires manufacturers of these products to pay compensatory royalties to copyright holders,[316] and mandates that all such products include a Serial Copy Management System ("SCMS").[317] The SCMS "sends, receives, and acts upon information about the generation and copyright status of the files that it plays."[318] More specifically, the SCMS prevents digital audio equipment from making a chain of high

307. *Id.*
308. *Id.* at 423, 425.
309. *Id.* at 438.
310. *Id.* at 439-40.
311. *Id.* at 442.
312. 180 F.3d 1072, 1079 (9th Cir. 1999).
313. *Diamond Multimedia*, 180 F.3d at 1075.
314. Yu, *supra* note 13, at 706; *see also* Jennifer Norman, *Staying Alive: Can the Recording Industry Survive Peer-to-Peer*, 26 COLUM. J.L. & ARTS 371, 380 (2003).
315. 17 U.S.C.A. § 1008 (West 2006).
316. § 1003(a).
317. § 1002(a).
318. *Diamond Multimedia*, 180 F.3d at 1075.

quality digital copies; in other words, the user can make as many copies of an original recording as he wishes, but cannot make copies of copies.[319]

The district court agreed that the Rio failed to comply with the AHRA because it did not include the SCMS, but denied RIAA's request for a preliminary injunction.[320] On appeal, the Ninth Circuit held that the lower court erred in finding that the Rio was covered by AHRA because, in order to be a "digital audio recording device," the Rio must be able to reproduce a "digital music recording" either "directly" or "from a transmission."[321] The court further found that computer hard drives are not digital audio recording devices subject to the AHRA.[322]

Relying on *Sony Corporation of America v. Universal City Studios, Inc.*,[323] the court then went on to hold that, under the fair use doctrine, the Rio was not an infringing device.[324] "The Rio merely makes copies in order to render portable, or "space-shift," those files that already reside on a user's hard drive. Such copying is paradigmatic noncommercial personal use entirely consistent with the purposes of the [Copyright] Act."[325]

In sum, there is no bright-line test for determining what constitutes fair use, nor is there a blanket rule that all personal use is fair. But on a case-by-case basis, courts have decided that certain personal uses, including time-shifting and space-shifting, constitute fair and noninfringing use.

b. Did Sony's Copy-Prevention Software Allow Fair Use?

Up to this point, the DRM used by record labels has been "largely skewed in favor of the content owner at the expense of the consumer."[326] Critics have called these systems "too draconian" because of the limitations they place on consumers' ability to play music.[327] In other words, the recording industry has "los[t] sight of the fact that 'both . . . [the copyright owner and the consumer] have rights that need to be protected.'"[328]

With its copy-prevention software, Sony was attempting to strike this balance between protecting its intellectual property and allowing

319. Yu, *supra* note 13, at 707.
320. *Diamond Multimedia*, 180 F.3d at 1081.
321. *Id.* at 1081; *See* 17 U.S.C.A. § 1001(1), (3).
322. *Diamond Multimedia*, 180 F.3d at 1078.
323. 464 U.S. 417 (1984).
324. *Diamond Multimedia*, 180 F.3d at 1079.
325. *Id.* (citation omitted).
326. *Digital Rights Management (DRM): Media Companies' Next Flop?*, *supra* note 294.
327. *Id.*
328. *Id.* (third alteration in original) (quoting Kendall Whitehouse, Senior Director of Advanced Technology Development at the Wharton School of the University of Pennsylvania).

"responsible personal use by fans."[329] Generally, the software allowed a consumer to do the following with his purchased music: (i) save one copy of the CD on his hard drive; (ii) play the CD on his computer using certain media players; (iii) download the CD to certain portable devices; and (iv) burn three backup copies of the CD.[330] In addition, the MediaMax software allowed consumers to email tracks to friends who could listen to them for ten days.[331] Thus, the copy-prevention software was intended to allow users to space-shift their music for personal use (*i.e.*, listen to it on a computer, CD, or portable player), and to share music with friends, but not "'giv[e] it away forever.'"[332]

While this may have been Sony's intention, it was not the reality. The content on the copy-protected CDs could only be transferred to *certain* media players and portable devices (*i.e.*, those using Sony or Microsoft products), and could *not* be transferred to an iPod device or iTunes media player.[333] Given that the iPod is the dominant portable device and that iTunes is one of the most popular media players,[334] many purchasers of Sony's copy-protected CDs were denied the right to "space-shift" their music.

As discussed above, in *Recording Industry Association of America v. Diamond Multimedia Systems, Inc.*, the court specifically held that space-shifting legally purchased music to a portable MP3 player is permitted under the fair use doctrine.[335] It is true that "there is no unqualified right to access works on any particular machine or device of the

---

329. *Id.*

330. The exact parameters of what activity was prohibited by the software were spelled out in the EULA. It said:

> This CD contains technology that is designed to prevent users from making certain, unauthorized uses of the DIGITAL CONTENT, including, without limitation, the following: (1) making and storing more that one (1) copy of the DIGITAL CONTENT in each available file format on the hard drive of YOUR COMPUTER; (2) accessing the DIGITAL CONTENT on YOUR COMPUTER (once you have installed a copy of it on the hard drive of YOUR COMPUTER) using a media player that is not an APPROVED MEDIA PLAYER; (3) transferring copies of the DIGITAL CONTENT that reside on the hard drive of YOUR COMPUTER on to portable devices that are not APPROVED PORTABLE DEVICES; (4) burning more than three (3) copies of the DIGITAL CONTENT stored on YOUR COMPUTER (ATRAC OpenMG file format only) onto AtracCDs; (5) burning more than three (3) copies of the DIGITAL CONTENT onto recordable compact discs in the so-called "Red Book"-compliant audio file format; and (6) burning more than three (3) backup copies of this CD (using the burning application provided on the CD) onto recordable CDs and burning or otherwise making additional copies form the resulting backup copies.

Melcon Complaint, *supra* note 70, Ex. B.

331. Snider, *supra* note 70; Halderman, *supra* note 65, at 6.

332. Snider, *supra* note 70 (quoting William Whitmore of SunnComm).

333. Sony Complaint, *supra* note 68, ¶¶ 2, 24.

334. *Id.* ¶ 24; Daniel Greenberg, *Chasing Apple's Dominant iPod*, WASH. POST, Oct. 17, 2004, at F06; WebSiteOptimization.com, Apple's iTunes Player Climbs Streaming Media Charts, Mar. 15, 2006, http://www.websiteoptimization.com/bw/0603/.

335. *Diamond Multimedia*, 180 F.3d at 1079.

user's choosing."[336] However, as Dr. Richard Gooch, the Deputy Director of Technology for IFPI,[337] recently said: "[u]sers should be free to select among a wide range of devices and services from different suppliers while being safe in the knowledge that these will work properly together."[338]

Here, users were denied the right to choose from a wide variety of devices and were instead forced to listen to their copy-protected CDs on a portable device that was compatible with Sony or Microsoft products. For the significant number of customers whose portable device was an iPod, this meant they either had to go out and spend a few hundred dollars to purchase a new MP3 player or they had to accept that the content on their copy-protected CD could not be space-shifted.[339] This was not an acceptable choice. Accordingly, Sony went too far in attempting to protect its copyrighted works, and as a result, impinged on its customers' right to fair use.

### *B. Potential Liability Under DMCA*

Another issue raised by the Sony rootkit debacle concerns the Digital Millennium Copyright Act of 1998 (DMCA),[340] a federal statute that broadly prohibits the circumvention of DRM technology.[341] More specifically, the question is whether (i) Sony customers who attempted to remove the copy-protection software from their computers, and (ii) individuals who provided information as to how to remove the copy-protection software to the public, are potentially liable under the DMCA.

#### 1. The Background of the DMCA

In December, 1996, the World Intellectual Property Organization (WIPO) held a conference in Geneva, which led to the adoption of the WIPO Copyright Treaty.[342] "[T]he WIPO Copyright Treaty was created

336. JOINT REPLY, *supra* note 303, at 34 (quoting the 2000 recommendations of the Register of Copyrights, 65 Fed. Reg. 64556, 64569 (Oct. 27, 2000)).

337. The IFPI is the International Federation of Phonogram and Videogram Producers.

338. Gooch, *supra* note 294.

339. *Cf.* JOINT REPLY, *supra* note 303, at 34 (arguing that the fact that DVDs cannot be played on Linux operating systems is not a violation of fair use because "[c]opyright owners have never been legally required to enable access to their products from a multiplicity of platforms . . . . Over eighty million U.S. households now own a DVD player. DVD players can be purchased for less than fifty dollars and portable DVD players can be purchased for less than one hundred dollars."). The media companies are arguing that they should not have to make DVDs compatible with Linux systems because (i) most people do not have a Linux operated computer, and (ii) most people have a DVD player or could easily purchase one. *See id.* at 34-35. These arguments do not apply here: (i) most people have an iPod, not a Sony/Microsoft compatible MP3 player; (ii) most people do not have more than one MP3 player; and (iii) MP3 players are still relatively expensive. *See* Sony Complaint, *supra* note 68, ¶ 24 (describing iPod as "the dominant portable" MP3 player); Greenberg, *supra* note 334 (discussing the popularity of iPod and prices of rival MP3 players).

340. Digital Millennium Copyright Act, Pub. L. No. 105-304, 112 Stat. 2860 (1998) (codified in scattered sections of 5 U.S.C.A., 17 U.S.C.A., 28 U.S.C.A., and 35 U.S.C.A.).

341. *See* 17 U.S.C.A. § 1201.

342. Cohen, *supra* note 48, at 972.

to address the changing needs of copyright protection in a digital age," including digital rights management.[343] More specifically, the Treaty required contracting states to "provide adequate legal protection and effective legal remedies against the circumvention of effective technological measures that are used by authors in connection with the exercise of their rights under this Treaty or the Berne Convention."[344]

On October 12, 1998, Congress passed the DMCA, and President Clinton signed it into law.[345] Among other things, the DMCA is designed to implement the WIPO Copyright Treaty.[346] To that end, at the heart of the DMCA lies 17 U.S.C.A. section 1201(a)(1)(A), the anti-circumvention provision, which prohibits a person from "circumvent[ing] a technological measure that effectively controls access to a work protected under" the copyright statute.[347] This includes activity to "descramble a scrambled work, to decrypt an encrypted work, or otherwise to avoid, bypass, remove, deactivate, or impair a technological measure, without the authority of the copyright owner."[348] In addition, sections 1201(a)(2) and 1201(b)(1) of the DMCA, sometimes referred to as the "anti-trafficking provisions," preclude the designing, manufacturing, importing, offering to the public, or trafficking of any technology, service, or device produced to circumvent such technological measures.[349] Hence, a violation of the DMCA can occur even in the absence of copyright infringement.[350]

There are, however, seven narrow exemptions to the anti-circumvention provision of the DMCA, including for: (1) nonprofit libraries, archives, and educational institutions to gain access to copyrighted works to decide whether to acquire a copy of the work;[351] (2) law enforcement, intelligence, and other governmental entities to engages in any lawful investigative activities;[352] (3) reverse engineering of computer programs;[353] (4) encryption research;[354] (5) prevention of minors from accessing material on the Internet;[355] (6) protection of personally identifying information;[356] and (7) security testing.[357] The DMCA further pro-

343. *Id.*
344. WIPO Copyright Treaty, art. 11, Apr. 12, 1997, S. Treaty Doc. No. 105-17, 36 I.L.M. 65.
345. Digital Millennium Copyright Act, 112 Stat. at 2860 (enacting the DMCA); Statement by President William J. Clinton upon signing H.R. 2281, 1998 U.S.C.C.A.N. 671 (Oct. 28, 1998) (signing the DMCA into law).
346. Digital Millennium Copyright Act, 112 Stat. at 2860.
347. 17 U.S.C.A. § 1201(a)(1)(A).
348. § 1201(a)(3)(A).
349. § 1201(a)(2)(A), (3)(A).
350. *See* Cohen, *supra* note 48, at 976.
351. § 1201(d).
352. § 1201(e).
353. § 1201(f)(1)-(4).
354. § 1201(g).
355. § 1201(h).
356. § 1201(i).
357. § 1201(j).

vides that "the Librarian of Congress, upon the recommendation of the Register of Copyrights," is required to promulgate regulations every three years, exempting from the anti-circumvention provision, individuals who would otherwise be "adversely affected" in "their ability to make noninfringing uses."[358] The current regulations, which were adopted by the Librarian in 2003, carve out exceptions for the following four classes of works: (1) compilations of lists of web sites that are blocked by filtering software; (2) computer programs protected by dongles that cannot be accessed due to damage, malfunction, or obsolescence; (3) computer programs and video games in obsolete formats; and (4) literary works in eBook format that are unavailable to disabled persons.[359]

In rulemaking years, like 2006, the Copyright Office solicits comments from interested parties regarding proposed exemptions.[360] This year, the Copyright Office received close to one hundred comments, some of which addressed the Sony rootkit incident.[361] In the spring of 2006, the Copyright Office held hearings regarding the proposed exemptions,[362] and it is scheduled to publish its final recommendation in October 2006.[363]

### 2. Did Sony Customers Violate the Anti-Circumvention Provisions of the DMCA By Removing the Copy-Prevention Software From Their Computers?

Once the news of the rootkit broke on the Internet, many Sony customers attempted to uninstall the copy-prevention software themselves or hired someone to do it for them.[364] Some expressed concern that, by doing so, these customers may have been violating the DMCA, namely the anti-circumvention provision set forth in 17 U.S.C. § 1201(a)(1)(A).[365] While these concerns are understandable, an analysis

---

358. 17 U.S.C.A. § 1201(a)(1)(B)-(C). In making this determination, the Librarian shall consider:

> (i) the availability for use of copyrighted works; (ii) the availability for use of works for nonprofit archival, preservation, and educational purposes; (iii) the impact that the prohibition on the circumvention of technological measures applied to copyrighted works has on criticism, comment, news reporting, teaching, scholarship, or research; (iv) the effect of circumvention of technological measures on the market for or value of copyrighted works; and (v) such other factors as the Librarian considers appropriate.

§ 1201 (a)(1)(C)(i)-(v).

359. 37 C.F.R. § 201.40; Joseph P. Liu, *Regulatory Copyright*, 83 N.C. L. REV. 87, 124 & n. 252 (2004).

360. U.S. COPYRIGHT OFFICE, COMMENTS ON ANTICIRCUMVENTION EXEMPTIONS, http://www.copyright.gov/1201/2006/comments/index.html (last visited Sept. 2, 2006).

361. *Id.* (follow "Comment" hyperlinks).

362. U.S. COPYRIGHT OFFICE, ANTICIRCUMVENTION RULEMAKING HEARINGS SCHEDULE, http://www.copyright.gov/1201/2006/index.html (last visited Sept. 2, 2006).

363. *Id.*

364. *See* Mook, *supra* note 128.

365. MFC-in-the-box, Sony's XCP Rootkit and the DMCA, Nov. 22, 2005, http://mhc.insidestretch.com/2005/11/22/sonys-xcp-drm-rootkit-and-the-dmca/; Declan McCullagh, *Perspective: Why They Say Spyware is Good for You*, CNET NEWS, Nov. 7, 2005, http://news.com.com/Why+they+say+spyware+is+good+for+you/2010-1071_3-5934150.html; Mark

of the DMCA indicates that the current exemptions to section 1201(a)(1) most likely would have shielded these customers from liability.

First, section 1201(j) provides an exemption for any "act of security testing," which means "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."[366] This exemption applies to Sony customers who, after learning about the security risks posed by the copy-prevention software, removed the files from their hard drives.

Second, individuals whose computers were affected by the MediaMax or XCP software also may have been able to invoke section 1201(i), the exemption relating to the protection of personally identifiable information. That exemption provides:

> Notwithstanding the provisions of subsection (a)(1)(A), it is not a violation of that subsection for a person to circumvent a technological measure that effectively controls access to a work protected under this title, if—
>
> (A) 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.[367]

Both the MediaMax and XCP software had "phone home" capabilities, meaning it communicated certain information from the user's computer to Sony's servers.[368] The information communicated to Sony included, among other things, the user's IP address.[369]

Computer users are assigned an IP address by their internet service provider or system administrator. No two IP addresses are the same. Although some users have dynamic IP addresses, many have static addresses that do not change over time. Thus, an IP address can be used to determine information about the computer user, including his name, address, etc.[370] In fact, this is exactly how the record companies have identified "John Doe" defendants in their litigation campaign against individual file-sharers.[371] Because an IP address constitutes "personally identifying information" (or, at the very least, is an avenue to personally identifi-

---

Russinovich, *Sony's Rootkit First 4 Internet Responds*, Nov. 6, 2005, http://www.sysinternals.com/blog/2005/11/sonys-rootkit-first-4-internet.html (see replies).

366. 17 U.S.C.A. § 1201(j)(1), (2).

367. § 1201(i)(1)(A).

368. Russinovich Affidavit, *supra* note 119, ¶ 14; Settlement Agreement, *supra* note 63, ¶ E.

369. Settlement Agreement, *supra* note 63, ¶ E.

370. Melcon Complaint, *supra* note 70, ¶ 31.

371. *See supra* Part I.A.2.

able information), section 1201(i) should have protected Sony's customers from liability under the DMCA.

In sum, section 1201(i) and (j) almost certainly would have shielded from liability Sony customers who uninstalled the copy-prevention software from their hard drives. Yet, as explained in the next section, the current exemptions to the DMCA may not be broad enough to protect everyone involved in the Sony rootkit debacle from liability.

3. Did Security Researchers Violate the Anti-Trafficking Provisions of the DMCA by Informing the Public About Sony's Copy-Prevention Software?

When Mark Russinovich published his findings about the Sony rootkit on the Internet, he apparently was not concerned about or not aware of the potential legal exposure created by the DMCA. Others were, however. Professor Felten and Alex Halderman, both of whom had previously been threatened with DMCA suits, said that they had uncovered the problem with Sony's copy-prevention software about a month before Mr. Russinovich broke the news, but did not disclose it because they were worried about a lawsuit.[372] Those fears appear to have been well-founded.

a. Liability Under the Anti-Trafficking Provisions of the DMCA

In addition to prohibiting the circumvention of DRM and other technological measures aimed at protecting copyrighted material, certain provisions of the DMCA also make it illegal to traffic in a technology, service, or device intended to circumvent such technological measures. Subsection 1201(a)(2) provides:

> No person shall manufacture, import, offer to the public, provide, or otherwise traffic in any technology, product, service, device, component, or part thereof, that—(A) is primarily designed or produced for the purpose of circumventing a technological measure that effectively controls access to a work protected under this title; (B) has only limited commercially significant purpose or use other than to circumvent a technological measure that effectively controls access to a work protected under this title; or (C) is marketed by that person or another acting in concert with that person with that person's knowledge for use in circumventing a technological measure that effectively controls access to a work protected under this title.[373]

Similarly, subsection 1201(b)(1) provides:

372. Comment of Edward W. Felten & J. Alex Halderman, Dec. 1, 2005, at 7 [hereinafter Felten Comment], *available at* http://www.copyright.gov/1201/2006/comments/mulligan_felten.pdf.

373. 17 U.S.C.A. § 1201(a)(2).

> No person shall manufacture, import, offer to the public, provide, or otherwise traffic in any technology, product, service, device, component, or part thereof, that—(A) 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; (B) has only limited commercially significant purpose or use other than to circumvent 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; or (C) is marketed by that person or another acting in concert with that person with that person's knowledge for use in 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.[374]

Although both subsections prohibit trafficking in a circumvention technology, the focus of section 1201(a)(2) is circumvention of technologies designed to prevent access to a work, and the focus of section 1201(b)(1) is circumvention of technologies designed to permit access to a work but prevent copying of the work or some other act that infringes a copyright.[375]

Since the DMCA was enacted in 1998, a few courts have interpreted the anti-trafficking provisions of that statute. One of the earliest decisions was *Universal City Studios, Inc. v. Corley*.[376] In that case, several movie studios filed a lawsuit against two website owners who, among other things, posted links to other websites that offered for download a computer software program called DeCSS.[377] One of the purposes of DeCSS was to circumvent CSS, an encryption system used to prevent illegal copying of DVDs.[378] "CSS-protected motion pictures on DVDs may be viewed only on players and computer drives equipped with licensed technology that permits the devices to decrypt and play—but not to copy—the films."[379]

The lower court found that by posting links to DeCSS on their websites, defendants had violated section 1201(a)(2) of the DMCA because they offered and provided to the public a technology, *i.e.*, DeCSS, that is "primarily designed or produced for the purpose of circumventing a technological measure," *i.e.*, CSS.[380] Accordingly, the court entered a

374. § 1201(b)(1).
375. S. REP. NO. 105-190, at 11-12 (1998).
376. 273 F.3d 429 (2d Cir. 2001). The lower court decision is reported at 111 F. Supp. 2d 294 (S.D.N.Y. 2000).
377. Corley, 273 F.3d at 435-36.
378. *Id.* at 436-37.
379. Universal City Studios v. Reimerdes, 111 F. Supp. 2d 294, 303 (S.D.N.Y. 2000).
380. § 1201(a)(2)(A); *Reimerdes*, 111 F. Supp. 2d at 316-17.

permanent injunction against defendants, which the Second Circuit upheld.[381]

More recently, in *Davidson & Associates v. Jung*,[382] the Eighth Circuit faced the question whether the anti-trafficking provisions of the DMCA had been violated in connection with certain computer game software. In that case, plaintiff Blizzard Entertainment ("Blizzard"), the owner of copyrights in computer game software, launched Battle.net, a 24-hour online gaming service available only to people who purchase Blizzard's computer games.[383] The Battle.net service facilitates multiple-player games, meaning users can "create and join multi-player games that can be accessed across the Internet, . . . chat with other potential players, . . . record wins and losses and save advancements in an individual password-protected game account, and . . . participate with others in tournament play featuring elimination rounds."[384]

Defendants were software programmers who formed a group called the "bnetd project."[385] The bnetd project established a website and offered an alternative service to Battle.net, which also "allow[ed] gamers unable or unwilling to connect to Battle.net to experience the multi-player features of Blizzard's games."[386] In order for bnetd.org to work with Blizzard games, defendants had to reverse engineer the game software, including the technological measures intended to prevent illicit copying.[387]

Blizzard sued defendants alleging, among other things, violations of the DMCA's anti-circumvention and anti-trafficking provisions.[388] The court held that, by reverse engineering the Blizzard game software, defendants violated section 1201(a)(1)'s circumvention proscription, and that no exemption applied.[389] The court also determined that defendants were in violation of section 1201(a)(2) because they provided to the public a service whose primary purpose "was to avoid the anti-circumvention restrictions of the game and to avoid the restricted access to Battle.net."[390] Accordingly, the district court granted summary judgment in favor of Blizzard on these claims, and the Eighth Circuit affirmed.[391]

---

381. *Corley*, 273 F.3d at 434, 459-60.
382. 422 F.3d 630 (8th Cir. 2005).
383. *Davidson*, 422 F.3d at 633.
384. *Id.*
385. *Id.* at 635.
386. *Id.*
387. *Id.* at 636.
388. *Id.* at 637.
389. *Id.* at 640-41.
390. Davidson & Assocs., Inc. v. Internet Gateway, 334 F. Supp. 2d 1164, 1186 (E.D. Mo. 2004).
391. 422 F.3d at 640-41, *aff'g* 334 F. Supp. 2d 1164 (E.D. Mo. 2004).

Although security researchers like Messrs. Russinovich, Felten, and Halderman have not manufactured any sort of product or device to circumvent Sony's copy-prevention software, all three have provided the public with information about the manner in which this software operates, the dangers it poses, and how it can be removed from one's hard drive. In light of the decisions in *Corley* and *Davidson*, such conduct arguably falls within the purview of the DMCA's anti-trafficking provisions because it is a *service* that is *being provided or offered to the public* primarily for the purpose of *circumventing a technological measure* that prevents access to a copyrighted work. Indeed, Professor Felten and Alex Halderman themselves are concerned about the legality of their conduct. Not only did they choose not to disclose their research about Sony's copy-prevention software, but they also have asked the Copyright Office to promulgate a regulatory exemption to the DMCA to protect their activities in the future.

b. Proposed Exemptions to the DMCA

As mentioned above, 2006 is a rulemaking year under the DMCA, which means the Copyright Office is considering various proposed exemptions to the anti-circumvention provisions of the statute. Among the numerous submissions received by the Copyright Office were two that addressed, at least in part, the situation raised by the Sony rootkit debacle: (1) the Comments of Edward Felten and J. Alex Halderman, submitted by their legal representatives from the Samuelson Law, Technology and Public Policy Clinic at Boalt Hall; and (2) the Comments of the Computer and Communications Industry Association and Open Source and Industry Alliance (collectively "CCIA").[392]

Generally, these two groups requested "an exemption to § 1201(a)(1)(A) for sound recordings and audiovisual works distributed in compact disc format and protected by technological measures that impede access to lawfully purchased works by creating or exploiting security vulnerabilities that compromise the security of personal computers."[393] They contend that such an exemption is necessary to allow consumers to enjoy their purchased music without threatening the security of their computers, and so that individuals like Messrs. Felten and Halderman can engage in security research.[394]

392. U.S. COPYRIGHT OFFICE, COMMENTS ON ANTICIRCUMVENTION EXEMPTIONS, http://www.copyright.gov/1201/2006/comments/index.html.

393. Felten Comment, *supra* note 372, at 1. The exemptions proposed by the two groups are essentially identical and, thus, will be discussed together.

394. *Id.* at 6-7; *see also* Public Hearing on Exemption to Prohibition on Circumvention of Copyright Protection Systems for Access Control Technologies, U.S. Copyright Office, Mar. 31, 2006, at 130-33, *available at* http://www.copyright.gov/1201/2006/hearings/transcript-mar31.pdf.

Numerous organizations, including the RIAA, submitted a joint response to the comments proposing new exemptions to the DMCA.[395] The joint response asserted that the exemption proposed by the Felten and CCIA groups was unnecessary because, *inter alia*, the conduct about which they were concerned was already exempted under sections 1201(i) and (j).[396] As discussed previously, this most likely is true with respect to Sony customers who removed the copy-prevention software from their computers.[397]

As currently drafted, however, the 1201(j) and (i) exemptions probably would not protect security researchers who provide information to the public from liability under the anti-trafficking provisions of the DMCA. Section 1201(j) provides, for example, that

> [i]n determining whether a person qualifies for the exemption under paragraph (2), the factors to be considered shall include—(A) whether the information derived from the security testing was used solely to promote the security of the owner or operator of such computer, computer system or computer network, or shared directly with the developer of such computer, computer system, or computer network; and (B) whether the information derived from the security testing was used or maintained in a manner that does not facilitate infringement under this title or a violation of applicable law other than this section, including a violation of privacy or breach of security.[398]

Here, the information that Messrs. Felten, Halderman, and Russinovich derived from security testing was not used *solely* to promote the security of their own computers, but also was used to promote the security of other Sony customers' computers. Moreover, although the purpose of disseminating such information is to promote the security of personal computers, there is no guarantee that such information will not be used to facilitate infringement. Thus, as discussed in Part IV of this Article, the Copyright Office should adopt a narrowly-tailored exemption to protect those engaged in security research from liability under the DMCA.

## IV. RECORD COMPANIES SHOULD CONTINUE TO USE DRM, BUT NOT AT THE EXPENSE OF SECURITY RESEARCHERS OR CONSUMERS

Despite the complications caused by the Sony rootkit debacle, the recording industry should continue to pursue DRM technology to prevent the illicit copying of CDs. The recording industry has a right to protect its intellectual property. Unlike the on-line file sharing battle, there are no secondary infringers like Napster or Grokster that could be targeted,

---

395. JOINT REPLY, *supra* note 303, at 1.
396. *Id.* at 20-21.
397. *See supra* Part III.B.2.
398. § 1201(j)(3).

and suing direct infringers is not practical because it would be extremely difficult, if not impossible, to identify individual CD burners. DRM, therefore, is still the industry's best option. In order for future attempts at DRM to succeed, however, lawmakers and record companies alike must strive to balance the interest of copyright owners against the rights of consumers.

### *A. What Should the Lawmakers Do?*

This article has analyzed many legal issues raised by the rootkit incident, including Sony's potential liability, as well as the potential liability of consumers and researchers under the DMCA. As to the former, there are federal and state laws available to address and remedy Sony's conduct.[399] With respect to the latter, the current exemptions to the DMCA are not sufficient to protect security researchers from liability and, thus, the Copyright Office should adopt a new exemption.

However, the exemption proposed by the Felten and CCIA groups—"for sound recordings . . . distributed in compact disc format and protected by technological measures that impede access . . . by creating or exploiting security vulnerabilities that compromise . . . personal computers"[400]—is far too broad. First and foremost, it is not limited in any way to security researchers, so it would permit anyone who believed a copy-protected CD posed some type of security risk to circumvent the technology. Nor does the proposed exemption attempt to define "security vulnerabilities," so some people might interpret that term very broadly to justify the circumvention of access controls. Undoubtedly, a vague and overly broad exemption like this would facilitate copyright infringement and seriously undermine the purpose served by section 1201 (a)(1)(A).

Instead, the Copyright Office should adopt a narrowly-tailored Security Research Exemption that tracks the language of section 1201(g)'s exemption for encryption research. Section 1201(g), for example, provides a relatively straightforward definition of "encryption research" that puts the public on notice of what activities fall within the exemption.[401] Section 1201(g) further provides that it is not a violation of section 1201(a)(1)(A) "for a person to circumvent a technological measure . . . in the course of an act of *good faith* encryption research *if . . . such an act is necessary to conduct such encryption research . . .*."[402] This type of

399. *See supra* Part III.A (discussing Sony's liability under the CFAA and Texas Spyware Statute). This is not to suggest that Congress should not enact a federal spyware statute. While such legislation probably is unnecessary in this case, it apparently is critical to address other serious problems facing consumers and businesses today. *See, e.g.*, Patterson, *supra* note 171, at 256-57; Blakley, *supra* note 173, at 40.

400. Felten Comment, *supra* note 372, at 1. The exemptions proposed by the two groups are essentially identical, and thus, will be discussed together.

401. § 1201(g)(1)(A).

402. § 1201(g)(2) (emphasis added).

limiting language, which is not found in the current security testing exemption, should be included in the proposed Security Research Exemption, so that the underlying copyrighted works can be accessed if necessary for the research.

Additionally, section 1201(g)'s "Factors in Determining Exemption" would be equally applicable to a Security Research Exemption. The first asks "whether the information derived from the encryption research was disseminated, and if so, whether it was disseminated in a manner reasonably calculated to advance the state of knowledge or development of encryption technology, versus whether it was disseminated in a manner that facilitates infringement under this title . . . ."[403] Before applying the Security Research Exemption, this type of inquiry would be appropriate to ensure that information was being disseminated to the members of the public to notify them of a valid security risk, and not simply to educate them on how to circumvent certain access controls.[404]

Similarly, section 1201(g) asks "whether the person is engaged in a legitimate course of study, is employed, or is appropriately trained or experienced, in the field of encryption technology."[405] A factor like this would ensure that only legitimate security researchers would be shielded by the exemption. Section 1201(g) finally considers "whether the person provides the copyright owner of the work to which the technological measure is applied with notice of the findings and documentation of the research . . . ."[406] Again, a notice provision should also be included in the proposed Security Research Exemption, thus giving the copyright owner an opportunity to address the problem itself instead of having it revealed by a third party as occurred in the Sony incident.

The proposed exemption outlined above would ensure that legitimate security researchers could devote their time to protecting our nation's computing systems and the people who use those systems, rather than worrying about whether disseminating important security information might expose them to a lawsuit under the DMCA. Moreover, this exemption is sufficiently narrow to minimize the risk that individuals could improperly invoke it in order to circumvent DRM systems for illicit purposes. While adoption of the proposed Security Research Exemption is recommended at this time in light of recent events, the ultimate goal is for record companies to adjust their approach and attitude

403. § 1201(g)(3)(A).

404. While Felten and Halderman's work is primarily focused on exposing security vulnerabilities created by various DRM systems, there are some instances where they seem simply to be instructing the public on circumvention techniques. *See, e.g.*, Halderman & Felten, *supra* note 62, at 6 (explaining how to bypass XCP's temporary protection measure by "kill[ing] the installer process" or "us[ing] a ripping or copying program that locks the CD tray," even though there is no indication that this temporary protection measure poses security risks to the user).

405. § 1201(g)(3)(B).

406. § 1201(g)(3)(C).

toward copy-protecting CDs, so as to avoid another Sony rootkit debacle in the future.

*B. What Should the Record Companies Do?*

Record companies need to take a different approach to copy-protecting CDs. First, they need to invest the time and resources necessary to ensure their copy-prevention systems do not pose any sort of security threat to their customers. The record labels and the software designers must make security a priority so consumers can feel confident that playing copy-protected CDs on their computers will not pose a risk to their operating systems. Moreover, before releasing CDs with copy-protection software, all record companies should do what Sony is required to do by the Settlement Agreement in the Consolidated Action: have the software analyzed by an independent, third-party and get an opinion that installation and use of the software would create no security vulnerabilities for users.[407]

Second, it is vital that record companies provide consumers with sufficient notice that CDs contain anti-piracy technology. Record labels not only should include conspicuous warnings on the CDs, but they should widely publicize the fact that certain copy-protected CDs are going to be released. Additionally, consumers must be fully informed about the nature of the DRM (*i.e.*, what it does, how it operates, etc.). That information, of course, should be included in the EULA, but also should be made easily available to customers, for example by posting it on the label's website. Indeed, one reason Apple has been successful with its use of DRM in iTunes music is because "Apple is above the board . . . ."[408]

Third, while it would be impossible to ensure that copy-protected CDs can be listened to on *any* device, record companies must develop DRM systems that take into account the reality of today's technological landscape. Specifically, a significant number of customers use portable music players, and Apple's iPod is by far the most popular of these devices. The bottom line is that if record companies release copy-protected CDs that are not compatible with iPods, and consumers are not aware of that at the time of purchase, music fans with be angry and/or will attempt to circumvent the DRM. While it is understandable that Sony would prefer its customers to listen to Sony CDs on a Sony MP3 player, that is simply not the reality of today's society. In other words, the record companies cannot use copy-protection as a means to promote their own portable devices. If record labels want to copy-protect CDs, they must accept that most customers will want to listen to those CDs on an iPod.

---

407. Settlement Agreement, *supra* note 63, ¶ IV.B.3(f).
408. *Digital Rights Management (DRM): Media Companies' Next Flop?*, *supra* note 294.

Finally, the sole purpose of any successful DRM system must be to prevent illicit copying, not to collect personal information or advertise. This is addressed in the Settlement Agreement in the Consolidated Action, but it does not go far enough. There, Sony agreed that, before releasing CDs with copy-prevention software, it will ensure that such software "make[s] a record only of the associated album title, artist, IP address from which the [Internet] connection was made, and certain non-personally identifiable information . . . ."[409] As discussed above, however, IP addresses are personally identifiable information. There is no reason record labels should be able to collect this information from individuals who are simply listening to CDs on their computers (as opposed to people who are illegally downloading music from the Internet). If record companies continue to gather such data, it will further erode customer confidence and undermine the chance of finding an approach to DRM that is acceptable to the entertainment industry and consumers.

## CONCLUSION

This latest chapter in the saga of the war on music piracy has forced the recording industry, lawmakers, and consumers to take a hard look at the issues surrounding the use of digital rights management to protect copyright owners. In this case, Sony clearly went too far in attempting to defend its intellectual property rights. As a result, it violated numerous laws and has subjected itself to very serious consequences, including several class action lawsuits, a criminal case in Texas, numerous government inquiries, and a public relations disaster.

The record companies nonetheless have a right to prevent illicit copying of their music, and, at least for the time being, digital rights management is the best way to accomplish that. In designing future DRM systems, the recording industry should take a lesson from Apple, who has made its iTunes DRM work by "think[ing] seriously about balancing the needs of content owners with those of consumers," and "attempt[ing] to satisfy both sides of the equation."[410] If the recording industry can do that and can develop DRM that satisfies the requirements outlined in this article, consumers would learn to accept the copy-protection technology and would adapt their music consumption habits accordingly.

409. Settlement Agreement, *supra* note 63, ¶ IV.B.3(g).
410. *Digital Rights Management (DRM): Media Companies' Next Flop?*, *supra* note 294.