Title:
The Magnificence of the Disaster: Reconstructing the Sony Bmg Rootkit Incident

Author:
Mulligan, Deirdre, University of California, Berkeley
Perzanowski, Aaron K., UC Berkeley School of Law

Publication Date:
09-19-2008

Series:
Law and Technology Scholarship

Publication Info:
Law and Technology Scholarship, Berkeley Center for Law and Technology, UC Berkeley

Permalink:
http://escholarship.org/uc/item/0dx2g7xw

Keywords:
DRM, TPM, copy protection, HCI-Sec, rootkit, copyright, DMCA, security

Abstract:
Late in 2005, Sony BMG released millions of Compact Discs containing digital rights management technologies that threatened the security of its customers' computers and the integrity of the information infrastructure more broadly. This Article aims to identify the market, technological, and legal factors that appear to have led a presumably rational actor toward a strategy that in retrospect appears obviously and fundamentally misguided.

The Article first addresses the market-based rationales that likely influenced Sony BMG's deployment of these DRM systems and reveals that even the most charitable interpretation of Sony BMG's internal strategizing demonstrates a failure to adequately value security and privacy. After taking stock of the then-existing technological environment that both encouraged and enabled the distribution of these protection measures, the Article examines law, the third vector of influence on Sony BMG's decision to release flawed protection measures into the wild, and argues that existing doctrine in the fields of contract, intellectual property, and consumer protection law fails to adequately counter the technological and market forces that allowed a self-interested actor to inflict these harms on the public.

The Article concludes with two recommendations aimed at reducing the likelihood of companies deploying protection measures with known security vulnerabilities in the consumer marketplace. First, Congress should alter the Digital Millennium Copyright Act (DMCA) by creating permanent exemptions from its anti-circumvention and antitrafficking provisions that enable security research and the dissemination of tools to remove harmful protection measures. Second, the Federal Trade

Commission should leverage insights from the field of human computer interaction security (HCI-Sec) to develop a stronger framework for user control over the security and privacy aspects of computers.

THE MAGNIFICENCE OF THE DISASTER: RECONSTRUCTING THE SONY BMG ROOTKIT INCIDENT

By Deirdre K. Mulligan† & Aaron K. Perzanowski‡‡

---

† Clinical Professor of Law; Director, Samuelson Law, Technology & Public Policy Clinic; Director, Clinical Program, University of California, Berkeley School of Law (Boalt Hall).

‡‡ Associate, Fenwick & West LLP; J.D., University of California, Berkeley School of Law (Boalt Hall), 2006.

Much appreciation to Pamela Samuelson, Chris Hoofnagle, Fred B. Schneider, Matt Blaze, Edward Felten, Aaron Burstein, Ka-Ping Yee, Joseph Lorenzo Hall, Nathaniel Good, Fred von Lohmann, Jennifer M. Urban, Jack I. Lerner, the participants at the Copyright, DRM Technologies, and Consumer Protection Conference, and the TRUST (The Team for Research in Ubiquitous Secure Technology) Industrial Advisory Board members for insight, comment, and discussion; Edward Felten and J. Alex Halderman for giving us the opportunity to advise them on legal aspects of their research; Sara Adibisedeh, Azra Medjedovic, and Brian W. Carver for their assistance in providing that advice; Victoria Bassetti and others in industry for answering questions and providing helpful direction; and Sarala V. Nagala and Rebecca Henshaw for their able research. This paper would not have been possible without the support for interdisciplinary research provided by TRUST (The Team for Research in Ubiquitous Secure Technology), which receives support from the National Science Foundation (NSF award number CCF-0424422). Finally, the authors wish to thank Rebecca M. Fisher for providing the inspiration for the title of this article.

I. INTRODUCTION

Late in 2005, as many as two million[1] computer users learned that software unknowingly installed on their machines effectively ceded control of their computers and data to any enterprising hacker with the necessary ill intent. This software tool, known as a rootkit, enabled a host of attacks on individual users and both private and public network infrastructure. But the rootkit, a tool rarely employed by legitimate software developers,[2] was not installed by a virus attached to unscanned e-mails, nor was it bundled with adware developed by a disreputable vendor. It was instead distributed by Sony BMG Music Entertainment (Sony BMG), the world's second largest record label,[3] on millions of Compact Discs (CDs) sold to an unsuspecting public. The unwitting recipients of this software, Sony BMG's own customers, did no more than attempt to listen to lawfully purchased music on their computers.

---

1. Jefferson Graham, *Sony to Pull Controversial CDs, Offer Swap*, USA TODAY, Nov. 15, 2005, at 1B; Tom Zeller Jr., *Sony BMG Stirs a Debate Over Software Used to Guard Content*, N.Y. TIMES, Nov. 14, 2005, at C1.

2. Rootkits have been used in some instances by anti-virus software developers to protect their software from attack, but this incorporation of a rootkit into otherwise legitimate software sparked significant debate. *See* MCAFEE, ROOTKITS, PART 1 OF 3: THE GROWING THREAT (2006), http://download.nai.com/products/mcafee-avert/WhitePapers/AKapoor_Rootkits1.pdf.

3. Bertelsmann.com, BMG—A Passion for Music, http://www.bertelsmann.com/bertelsmann_corp/wms41/bm/index.php?ci=26&language=2 (last visited Sept. 6, 2007).

By the time the Sony BMG rootkit found its way to store shelves, CD-based copy protection schemes were nothing new. A variety of protection measures had been introduced on previous major label releases.[4] Although they differed in technological detail, these measures all aimed to disable or limit the ability of customers to access and copy music contained on CDs.

XCP, a CD-based protection measure developed by First4Internet and distributed by Sony BMG,[5] initially appeared to be no different than its predecessors. XCP created generally unwanted and unexpected restrictions on the ability to use lawfully purchased CDs. But in October of 2005, after CDs protected by XCP had been on the market for several months, computer engineer and security expert Mark Russinovich discovered that XCP incorporated a rootkit.[6] While Russinovich was not the first security researcher to uncover problems with Sony BMG's protection measures, he was the first to publicly disclose the presence of the rootkit because of the pall hanging over research in this field.[7] A blog post authored by Russinovich, and the media response it prompted,[8] alerted the public to the presence of the rootkit, offering the first glimpses into the potential security disaster enabled by Sony BMG's DRM.

As the public learned in the wake of Russinovich's disclosure, rootkits are software tools, frequently employed by developers of malicious soft-

---

4. *See, e.g.*, J. ALEX HALDERMAN, PRINCETON UNIVERSITY, ANALYSIS OF THE MEDIAMAX CD3 COPY-PREVENTION SYSTEM 1 (2003), ftp://ftp.cs.princeton.edu/techreports/2003/679.pdf; Evan Hansen, *Celine Dion Disc Could Crash European PCs*, ZDNET.CO.UK, Apr. 5, 2002, http://news.zdnet.co.uk/internet/0,1000000097,2107848,00.htm; John Leyden, *Marker Pens, Sticky Tape Crack Music CD Protection*, THE REGISTER, May 14, 2002, http://www.theregister.co.uk/2002/05/14/marker_pens_sticky_tape_crack/ (discussing how a Celine Dion CD can prevent Macs from rebooting); Tony Smith, *BMG to Replace Anti-Rip Natalie Imbruglia CDs*, THE REGISTER, Nov. 19, 2001, http://www.theregister.co.uk/2001/11/19/bmg_to_replace_antirip_natalie/.

5. The other three major labels—Universal Music Group, Warner Music Group, and EMI—were also First4Internet customers and had included XCP on certain pre-release materials. *See Sony Tests Technology to Limit CD Burning*, CNET.CO.UK, June 1, 2005, http://news.cnet.co.uk/digitalmusic/0,39029666,39189658,00.htm.

6. Mark's Blog, http://blogs.technet.com/markrussinovich/archive/2005/10/31/sony-rootkits-and-digital-rights-management-gone-too-far.aspx (Oct. 31, 2005, 11:04 PST).

7. *See infra* Part II.

8. *See* Mark's Blog, http://blogs.technet.com/markrussinovich/archive/2005/10/31/sony-rootkits-and-digital-rights-management-gone-too-far.aspx (Oct. 31, 2005, 11:04 PST); Paul F. Roberts, *Sony BMG Hacking Into CD Buyers' Computers*, FOXNEWS.COM, Nov. 03, 2005, http://www.foxnews.com/story/0,2933,174334,00.html; Francis Till, *Sony Plants Secret Controls on PCs*, NAT'L BUS. REV., Nov. 3, 2005, http://www.nbr.co.nz/home/column_article.asp?id=13371&cid=3&cname=Technology.

ware (malware),[9] that allow programmers to cloak files and processes, effectively hiding their existence and operation from both a computer's user and the machine's operating system.[10] These cloaking devices can facilitate any number of attacks on individual computers including coordinated offenses against websites, computer networks, and the internet itself. Once installed, a rootkit can be used to hide any code, regardless of its author's original purpose. As such, a hacker's ambition and imagination serve as the primary constraints on the destructive effects rootkits enable.[11]

While Sony BMG's customers first became aware of the dangers posed by the rootkit through media reports following Russinovich's October 31 announcement, the company was on notice that its product contained a rootkit, at the very least, four weeks earlier.[12] Finnish anti-virus software developer F-Secure contacted Sony BMG on October 4, 2005, alerting it to the presence of the rootkit.[13] Of course, First4Internet, as the developer that chose to incorporate the rootkit into its design, necessarily knew of its presence from the outset.

---

9. "Malware," short for malicious software, is a catch-all term that refers to any software designed to cause damage to a single computer, server, or computer network, and includes spyware, viruses, and other varieties of harmful software. Robert Moir, *Defining Malware: FAQ*, Oct. 1, 2003, http://www.microsoft.com/technet/security/alerts/info/malware.mspx; *see also* Adam Baratz & Charles McLaughlin, *Malware: What is It and How to Prevent It*, ARS TECHNICA, Nov. 11, 2004, http://arstechnica.com/articles/paedia/malware.ars.

10. GREG HOGLUND & JAMES BUTLER, ROOTKITS: SUBVERTING THE WINDOWS KERNEL 4, 8-10 (Addison-Wesley ed., 2005). Within the computer security community, there was some debate over the proper classification of XCP. Some deemed XCP a rootkit, while others applied the more ambiguous label of Potentially Unwanted Program. *See* MCAFEE, *supra* note 2, at 3.

11. Hackers could exploit the cloaking capabilities of the XCP rootkit simply by adding the prefix "sys" to the name of any files they chose to obscure. J. Alex Halderman & Edward W. Felten, *Lessons from the Sony CD DRM Episode*, *in* USENIX ASS'N, PROCEEDINGS OF THE 15TH USENIX SECURITY SYMPOSIUM 77, 18 (2006), *available at* http://itpolicy.princeton.edu/pub/sonydrm-ext.pdf (updated version).

12. Posting of Ed Felten to Freedom to Tinker, http://www.freedom-to-tinker.com/?p=937 (Nov. 30, 2005, 06:41 EST).

13. Steve Hamm, *Sony BMG's Costly Silence*, BUS. WK., Nov. 29, 2005, http://www.businessweek.com/technology/content/nov2005/tc20051129_938966.htm. In fact, according to Thomas Hesse, President of Sony BMG's Global Digital Business group, the alert from F-Secure was seen as a "routine matter" and "did not suggest that this software was anything but benign." *Id.* Even after F-Secure explained that the rootkit posed a major security risk, Sony BMG "didn't seem inclined to do anything about the CDs that were already in circulation" and "wanted to keep the problem quiet." *Id.*

Although Sony BMG claimed it was taking steps to address the issue,[14] it took no discernible action until Russinovich made the threat posed by the software a matter of public knowledge. And even then, Sony BMG attempted to downplay the importance of the rootkit discovery. As Thomas Hesse, Sony BMG's President of Global Digital Business, rhetorically asked, "Most people, I think, don't even know what a rootkit is, so why should they care about it?"[15]

Subsequently, in an attempt to mollify customers who had already purchased the infected CDs, Sony BMG offered tools to uninstall XCP.[16] But, as discussed *infra*, those tools did more harm than good.[17] In order to stem the tide of public outcry and potentially mitigate further damages, Sony BMG finally announced in mid-November its intention to recall the millions of XCP-infected CDs that remained in the retail chain.[18]

But even before the XCP recall was announced, the focus of scrutiny began to shift to Sony BMG's other preferred technological protection measure, SunnComm's MediaMax software. Unlike XCP, MediaMax did not employ a rootkit, but it did, however, introduce other significant security vulnerabilities.

MediaMax enabled a dangerous privilege escalation.[19] When installed, MediaMax created a directory called "SunnComm Shared" on the user's hard drive.[20] MediaMax set file permissions for this directory and its contents that enabled any user of the computer, whether she had administrator privileges or not, to read, modify, or delete the contents of the directory.[21] These permissions enabled a guest or remote user to replace the Media-

---

14. *Id.*

15. Neda Ulaby, *Sony Music CDs Under Fire from Privacy Advocates* (National Public Radio Program broadcast Nov. 4, 2005), *available at* http://www.npr.org/templates/story/story.php?storyId=4989260.

16. *Id.*

17. *See infra* notes 40-42 and accompanying text.

18. Tom Zeller, Jr., *CD's Recalled for Posing Risk to PC's*, N.Y. TIMES, Nov. 16, 2005, at C1.

19. *See* Wikipedia, Privilege Escalation, http://en.wikipedia.org/wiki/Privilege_escalation (last modified July 26, 2007) ("Privilege escalation is the act of exploiting a bug in an application to gain access to resources which normally would have been protected from an application or user. The result is that the application performs actions with a higher security context than intended by the application developer or system administrator.").

20. Jesse Burns & Alex Stamos, Information Security Partners, Media Max Access Control Vulnerability 1 (2005), http://www.eff.org/IP/DRM/Sony-BMG/MediaMaxVulnerabilityReport.pdf.

21. *Id.*

Max files with malicious code, either intentionally or inadvertently. When a user with administrator privileges later inserted a MediaMax disc, that malicious code would be activated, triggering all manner of potential attacks.[22] When SunnComm released a patch to address this threat, it created vulnerabilities similar to those caused by the XCP uninstall tool.[23]

Second and more fundamentally, MediaMax requires a user to possess administrator privileges simply to listen to a CD.[24] Requiring the use of an administrator account for such mundane purposes is both "unnecessary and dangerous."[25] Further compounding the security vulnerabilities created by MediaMax, one component of the software, a kernel process capable of altering any aspect of the system, is loaded into memory at all times, regardless of the presence of a MediaMax CD.[26]

Although the technological source of the security threats introduced by XCP and MediaMax differed, as researchers soon discovered, the creators of both protection measures exhibited other behavior typically associated with the purveyors of spyware. For example, the software End User License Agreements (EULAs) were rife with overreaching terms.[27] More troublingly, some of the EULA terms were simply untrue. The EULAs professed that the software would collect no information about the user or her computer,[28] as did assurances offered by SunnComm and Sony BMG on their websites[29] and in the press.[30] But despite the obvious sensitivity to

---

22. *Id* at 5.

23. Posting of Ed Felten to Freedom to Tinker, http://www.freedom-to-tinker.com/?p=942 (Dec. 7, 2005, 10:33 EST). The original patch was later replaced with one that avoided these problems. *Id*.

24. Posting of Ed Felten to Freedom to Tinker, http://www.freedom-to-tinker.com/?p=934 (Nov. 22, 2005, 03:51 EST).

25. *Id.*

26. *Id.*

27. The Sony BMG EULA terminated the rights of consumers if, *inter alia*, the original CD was stolen or the user filed for bankruptcy. The EULA also prohibited users from using the CD on an office computer, limited Sony BMG's liability to $5.00, and permitted Sony BMG to install and use backdoors in the copy protection software or media player to enforce its rights at any time, without notice. *See* Fred von Lohmann, *Now the Legalese Rootkit: Sony-BMG's EULA*, DEEP LINKS, Nov. 9, 2005, http://www.eff.org/deeplinks/archives/004145.php.

28. *See infra* text accompanying note 214.

29. Posting of J. Alex Halderman to Freedom to Tinker, http://www.freedom-to-tinker.com/?p=925 (Nov. 12, 2005, 12:30 EST).

30. *See, e.g.*, *Sony Sued Over Controversial CDs*, BBC NEWS, Nov. 22, 2005, http://news.bbc.co.uk/2/hi/technology/4459620.stm; Carrie Kirby, *Sony Gets an Earful Over CD Software; Program to Block Music Piracy Prompts Privacy, Security Worries*, S.F. CHRON., Nov. 11, 2005, at A1; Bruce Schneier, *Real Story of the Rogue Rootkit*,

privacy concerns reflected in the public statements issued by these companies,[31] the behavior of their protection measures told a different story. Each time a user listened to a MediaMax or XCP-protected CD, data were collected and transmitted to Sony BMG that included the user's IP address and a code corresponding to the particular CD title.[32]

Even if a user declined the Sony BMG EULA, thereby forgoing the ability to access the CD on a computer,[33] components of the MediaMax software were loaded temporarily onto the user's machine.[34] One component—a device driver that interfered with the ability of the computer's CD-ROM drive to copy data—was often permanently installed despite the computer owner's explicit refusal of the EULA terms.[35] This driver was loaded as part of the Windows kernel and could potentially "control virtually any aspect of the computer's operation."[36]

Compounding these concerns, both First4Internet and SunnComm, like many malware vendors, initially failed to provide users with an uninstaller to remove their software in its entirety.[37] After news of the XCP

WIRED, Nov. 17, 2005, http://www.wired.com/politics/security/commentary/securitymatters/2005/11/69601.

31. This sensitivity was likely due, in part, to earlier controversy over media players that report users' listening and viewing habits. After a security consultant discovered that the RealJukebox transmitted to RealNetworks a unique code corresponding to each customer and the names of the CDs to which each user listened, Real quickly issued a patch that disabled the transmission of this data. *See* Stuart J. Johnston, *RealPrivacy in the New Millennium?*, PCWORLD, Dec. 17, 1999, http://www.pcworld.com/article/id,14419-page,1/article.html.

32. Posting of Ed Felten to Freedom to Tinker, http://www.freedom-to-tinker.com/?p=923 (Nov. 10, 2005, 08:25 EST); Mark's Blog, http://blogs.technet.com/markrussinovich/archive/2005/11/04/more-on-sony-dangerous-decloaking-patch-eulas-and-phoning-home.aspx (Nov. 4, 2005 12:04 PST); posting of J. Alex Halderman to Freedom to Tinker, http://www.freedom-to-tinker.com/?p=925 (Nov. 12, 2005, 12:30 EST). At least in part, this software served a fairly benign function—namely, to update images and lyrics displayed while users listened to the CD.

33. If a user declined to accept the EULA, the CD was automatically ejected. Halderman & Felten, *supra* note 11, at 6.

34. *Id.* at 7; Posting of J. Alex Halderman to Freedom to Tinker, http://www.freedom-to-tinker.com/?p=925 (Nov. 12, 2005 12:30 EST); Posting of J. Alex Halderman to Freedom to Tinker, http://www.freedom-to-tinker.com/?p=936 (Nov. 28, 2005 14:23 EST).

35. Posting of J. Alex Halderman to Freedom to Tinker, http://www.freedom-to-tinker.com/?p=936 (Nov. 28, 2005 14:23 EST).

36. *Id.*

37. Posting of Ed Felten to Freedom to Tinker, http://www.freedom-to-tinker.com/?p=923 (Nov. 10, 2005, 08:25 EST); Halderman & Felten, *supra* note 11, at

rootkit broke, Sony BMG initially offered a software update that, in its words, "remove[d] the cloaking technology component that has been recently discussed in a number of articles."[38] Given the size of the update and its creation of new files on the user's computer, some suggested that the update simply replaced one cloaking mechanism with another.[39]

Once mounting public pressure demanded that uninstallers be provided, Sony BMG required customers to endure a Byzantine series of webpages, e-mails, and downloads before finally ridding themselves of XCP.[40] But Sony BMG's missteps were not limited to a lack of transparency and convenience. The web-based XCP uninstaller created security threats equal in magnitude to the rootkit it was intended to eliminate, permitting malicious code embedded in any website to attack unsuspecting customers who took steps to protect their machines by uninstalling the rootkit.[41] Days later, when SunnComm announced a web-based uninstaller for its Media Max DRM, it suffered from a nearly identical flaw.[42]

The temptation to write off Sony BMG's long and unfortunate series of missteps as a display of utter disregard, or even contempt, for user security and privacy is a strong one. Although the truth likely contains some traces of these simple narratives, any reconstruction of the rootkit incident that approaches reality reveals a more complicated story. Casting Sony BMG as a hapless licensee of flawed protection measures developed by irresponsible third party vendors does not shed any light on the possible

---

14; Posting of J. Alex Halderman to Freedom to Tinker, http://www.freedom-to-tinker.com/?p=925 (Nov. 12, 2005, 12:30 EST).

38. Sony BMG Music Entertainment, Software Updates/Plug-ins (Nov. 7, 2005), http://cp.sonybmg.com/xcp/english/updates.html, *available at* http://web.archive.org/web/20051107020216/http://cp.sonybmg.com/xcp/english/updates.html (last visited Sept. 6, 2007).

39. Posting of Ed Felten to Freedom to Tinker, http://www.freedom-to-tinker.com/?p=921 (Nov. 3, 2005, 07:35 EST).

40. Mark's Blog, http://blogs.technet.com/markrussinovich/archive/2005/11/09/sony-you-don-t-reeeeaaaally-want-to-uninstall-do-you.aspx (Nov. 9, 2005, 11:31 PST); Posting of Ed Felten to Freedom to Tinker, http://www.freedom-to-tinker.com/?p=923 (Nov. 10, 2005, 08:25 EST). SunnComm required similar steps. Posting of J. Alex Halderman to Freedom to Tinker, http://www.freedom-to-tinker.com/?p=931 (Nov. 17, 2005, 13:46 EST).

41. Posting of J. Alex Halderman & Ed Felten to Freedom to Tinker, http://www.freedom-to-tinker.com/?p=927 (Nov. 15, 2005 07:07 EST); Posting of J. Alex Halderman to Freedom to Tinker, http://www.freedom-to-tinker.com/?p=928 (Nov. 15, 2005, 15:46 EST).

42. Posting of J. Alex Halderman to Freedom to Tinker, http://www.freedom-to-tinker.com/?p=931 (Nov. 17, 2005, 13:46 EST).

failures of internal procedures to identify and prevent such mishaps and the misalignment of interests that cause them. Understanding the complex array of factors that contributed to Sony BMG's actions and reactions is an essential first step toward the adoption of policies and mechanisms to prevent similar incidents in the future.

This Article aims to identify the market, technological, and legal factors that appear to have led a presumably rational actor toward a strategy that in retrospect appears obviously and fundamentally misguided. Part II begins by considering the harm that resulted from Sony BMG's DRM strategy—both the damage to Sony BMG and its customers as well as the negative externalities imposed on a broad range of third parties. Part III examines potential market-based rationales that influenced Sony BMG's deployment of these DRM systems and reveals that even the most charitable interpretation of Sony BMG's internal strategizing demonstrates a failure to adequately value security and privacy. After taking stock of the then-existing technological environment that both encouraged and enabled the distribution of these protection measures in Part IV, we examine law, the third vector of influence on Sony BMG's decision to release flawed protection measures into the wild, in Part V. We argue that existing doctrine in the fields of contract, intellectual property, and consumer protection law fails to adequately counter the technological and market forces that allowed a self-interested actor to inflict such harms on the public.

Finally in Part VI, we present two recommendations aimed at reducing the likelihood of companies deploying protection measures with known security vulnerabilities in the consumer marketplace. First, we suggest that Congress should alter the Digital Millennium Copyright Act (DMCA) by creating permanent exemptions from its anti-circumvention and anti-trafficking provisions in order to enable security research and the dissemination of tools to remove harmful protection measures. Second, we offer promising ways to leverage insights from the field of human computer interaction security (HCI-Sec) to develop a stronger framework for user control over the security and privacy aspects of computers. The Federal Trade Commission (FTC), under its existing authority to protect consumers from deceptive and unfair practices, could develop best practices and regulations regarding the installation of software and the collection and transmission of information about users, their computers, and their actions. In addition, we recommend that the FTC explore the development of standards for security in the context of software and online data collection activities.

II. UNDISCLOSED HARM AND EXTERNALITIES

Before attempting to reconstruct the system of incentives that impelled Sony BMG to distribute the XCP and MediaMax protection measures, a clear accounting of both the actual and potential damage wrought by these technologies is in order. The harms flowing from the rootkit incident were varied and wide-reaching. The security flaws inherent in Sony BMG's DRM left users open to attack, and the DRM collected data about users' private activities without proper disclosure. Moreover, Sony BMG, as well as its artists, suffered damage to their reputation and bottom line as a result of the rootkit incident. But the effects of the rootkit extended well beyond the parties to these transactions. The rootkit incident threatened both the security of the network infrastructure and the future of DRM technology.

This Part briefly summarizes the harms suffered by the parties directly involved in the rootkit incident and then considers the broad social costs that resulted from Sony BMG's failure to fully account for the impact of its technology.

A. Direct Harm to Sony BMG, its Artists, and its Customers

The vulnerabilities created by Sony BMG's DRM gave rise to an array of potential abuses. The XCP rootkit permitted a hacker to write malicious code that, once installed on a user's computer, would run undetected so long as the name of the file containing that code began with the prefix "sys."[43] Similarly, the MediaMax privilege escalation allowed an attacker to replace code installed on users' machines and automatically executed upon insertion of a MediaMax disc.[44] Practically any malicious code authored by a hacker could take advantage of these general purpose security holes. The user's data could be altered, deleted, or even held for ransom; the machine could be rendered inoperable; a program could sniff sensitive passwords or collect financial records and other personal data; trade secrets and other corporate information could be collected; illegal data could be downloaded and stored on the user's machine. In short, these protection measures provided the means for remote attackers to take control of customers' computers.

Although these attacks represent worst case scenarios, the threats posed by Sony BMG's DRM were far from theoretical. Within days of the public rootkit announcement, malicious code leveraging the XCP protection scheme to hide from antivirus programs and system administrators

43. Halderman & Felten, *supra* note 11, at 18.
44. *Id.* at 17.

was spreading across the internet. A Trojan Horse[45] discovered early in November of 2005[46]—variously referred to as Backdoor.Ryknos,[47] Breplibot,[48] and Stinx-E[49]—attempted to take advantage of the cloaking capabilities of the rootkit.[50] Backdoor.Ryknos was transmitted via spam e-mail messages. Once on a user's system, it opened a back door to connect to an IRC[51] channel where the attacker could remotely control the user's system.[52] The remote attacker could download, delete, and execute files,[53] and send information about the compromised machine.[54] Antivirus and security software providers, already on the lookout for code intended to take advantage of the rootkit, quickly mobilized to identify and remove this Trojan. The high profile of the Sony BMG rootkit, coupled with this speedy response, likely discouraged others from attempting to further exploit the rootkit vulnerability.

To make matters worse, Sony BMG's surreptitious software installation and undisclosed data collection impeded the ability of computer users to make informed choices about security and privacy. The "phone home" feature of Sony BMG's DRM undermined customer privacy by collecting and transmitting information about users' interactions with protected CDs, including users' IP addresses.[55] But the EULA governing DRM-protected

---

45. Trojan Horses are programs that may appear benign or useful but in fact harbor malicious code. *See* MCAFEE, *supra* note 2, at 4.

46. Elia Florio, Symantec.com, Backdoor.Ryknos—Technical Details, http://www.symantec.com/security_response/writeup.jsp?docid=2005-111012-2048-99&tabid=2 (last updated Feb. 13, 2007).

47. *See* Elia Florio, Symantec.com, Backdoor.Ryknos—Summary, http://www.symantec.com/security_response/writeup.jsp?docid=2005-111012-2048-99&tabid=1 (last updated Feb. 13, 2007).

48. *See* Jarkko Turkulainen, F-Secure.com, *F-Secure Virus Descriptions: Breplbot.b*, http://www.f-secure.com/v-descs/breplibot_b.shtml (last updated Nov. 11, 2005); McAfee Threat Center, W32/Brepibot, http://vil.nai.com/vil/content/v_133091.htm#VirusChar (last updated Feb. 1, 2006).

49. *See* Sophos Threat Analysis, Troj/Stinx-E, http://sophos.com/virusinfo/analyses/trojstinxe.html (last visited Sept. 6, 2007).

50. Florio, *supra* note 47.

51. Internet Relay Chat ("IRC") is an open protocol used for text-based internet communication. *See generally* Wikipedia, Internet Relay Chat, http://en.wikipedia.org/wiki/Internet_Relay_Chat (last updated May 11, 2007).

52. Florio, *supra* note 46.

53. *Id.*; Turkulainen, *supra* note 48.

54. Florio, *supra* note 46.

55. In some instances the IP addresses collected by these protection measures could provide sufficient data to identify the user's location and identity. PETER ECKERSLEY ET

Sony BMG CDs explicitly disavowed any collection or dissemination of data related to customers or their computers. These misleading terms rendered Sony BMG customers incapable of offering informed consent to the data collection engaged in by XCP and MediaMax. Through this duplicity, Sony BMG deprived its customers of the ability to protect their own privacy.

Sony BMG also failed to disclose adequately the security failures of its DRM. Components of these measures were installed—sometimes permanently—before customers were confronted with the EULA terms.[56] The CD packaging, which was the only means of pre-installation notice, contained precious few indicia of the DRM contained within. The CD jewel cases featured the International Federation of the Phonographic Industry (IFPI) "Content Protected" logo on their spines[57] and a small nondescript "content protection grid" that provided general information and system requirements on their back covers.[58] These half-hearted disclosures failed to provide Sony BMG customers with fair warning of the security and privacy threats created by these DRM schemes or the scope of the limitations that they imposed on the use of the media.

Once the public became aware of the undisclosed costs of XCP and MediaMax, Sony BMG discovered that it was not insulated from the fallout of its own DRM strategy. CDs distributed with these protection measures experienced a steep drop-off in sales within some market segments. Later, the recall of millions of XCP and MediaMax discs led to significant expense and further lost sales opportunities.[59] In addition, Sony BMG

AL., ELECTRONIC FRONTIER FOUNDATION, SIX TIPS TO PROTECT YOUR ONLINE SEARCH PRIVACY (2006), http://www.eff.org/Privacy/search/searchtips.pdf.

56. Posting of J. Alex Halderman to Freedom to Tinker, http://www.freedom-to-tinker.com/?p=925 (Nov. 12, 2005, 12:30 EST); Posting of J. Alex Halderman to Freedom to Tinker, http://www.freedom-to-tinker.com/?p=936 (Nov. 28, 2005, 14:23 EST).

57. Electronic Frontier Foundation, A Spotters' Guide to XCP and SunnComm's MediaMax, http://www.eff.org/IP/DRM/Sony-BMG/guide.php (last visited Sept. 6, 2007).

58. *See* Figure 1, *infra* Part V; *see also* Sony BMG Music Entertainment, CD's Containing XCP Content Protection Technology, http://cp.sonybmg.com/xcp/english/titles.html (last visited Sept. 6, 2007).

59. Tom Zeller Jr., *Sony BMG to Recall Copy-Restricted CDs*, INT'L HERALD TRIB., Nov. 17, 2005, Finance at 13; Tom Zeller, Jr., *Technology; CD's Recalled For Posing Risk to PC's*, N.Y. TIMES, Nov. 16, 2005, at C1; *Sony BMG Recalls Discs With Flawed Protection System (Update4)*, BLOOMBERG.COM, Nov. 16, 2006, http://www.bloomberg.com/apps/news?pid=10000101&sid=aVhY_TwrFjQI&refer=japan; Paul Taylor, *Sony BMG Bows to Pressure*, FT.COM, Nov. 16, 2005, http://www.ft.com/cms/s/e9e41f72-56f4-11da-b98c-00000e25118c.html.

spent millions to settle the steady stream of lawsuits arising out of the rootkit incident.[60] Less quantifiably, the resulting backlash from artists and customers significantly damaged the reputations of Sony BMG and its parent corporations.

Potential customers who were aware of the existence and dangers posed by Sony BMG's protection measures steered clear of XCP discs. The sales history of *Get Right with the Man*, an XCP-infected album by Van Zant that was released some six months prior to the rootkit announcement, is emblematic of the online retail impact of the rootkit incident. On November 2, just two days after the initial public announcement of the rootkit, *Get Right with the Man* ranked at number 887 on the music charts at Amazon.com.[61] The next day, after Amazon user reviews alerted shoppers to the dangers posed by XCP, the album dropped to number 1,392.[62] By the Thanksgiving holiday weekend, the XCP recall was underway and the album plummeted to number 25,802.[63] In contrast, in retail environments in which customers had less immediate access to information about the dangers of XCP, sales of *Get Right with the Man* were relatively undisturbed.[64] Since brick and mortar retailers like Wal-Mart, the nation's leading seller of CDs,[65] do not facilitate the sort of customer feedback common to online retailers, this outcome is hardly surprising.

Once Sony BMG instituted the recall of the remaining XCP-protected discs, and later MediaMax CDs, its albums were largely unavailable for purchase. In total, Sony BMG recalled 4.7 million XCP-protected CDs, roughly 2.6 million of which had not yet been sold.[66] The XCP recall cost

---

60. *See infra* note 69.

61. Lorraine Woellert, *Sony's Escalating "Spyware" Fiasco*, BUS. WK., Nov. 22, 2005, http://www.businessweek.com/technology/content/nov2005/tc20051122_343542.htm?campaign_id=rss_tech.

62. *Id.*

63. *Id.*

64. John Borland, *Sony Sailing Past Rootkit Controversy*, CNET NEWS.COM, Nov. 21, 2005, http://news.com.com/Sony+sailing+past+rootkit+controversy/2100-1027_3-5965243.html.

65. Max Fraser, *The Day the Music Died*, THE NATION, Nov. 27, 2006, http://www.thenation.com/doc/20061211/fraser.

66. Hiawatha Bray, *New Security Flaw Vexes Sony BMG Piracy Battle*, BOSTON GLOBE, Dec. 8, 2005, http://www.boston.com/business/technology/articles/2005/12/08/new_security_flaw_vexes_sony_bmg_piracy_battle; Brian Garrity & Ed Christman, *Sony BMG Recalls Copy Protected CDs*, BILLBOARD.COM, Nov. 18, 2005, http://billboard.com/bbcom/news/article_display.jsp?vnu_content_id=1001524942. Even after the recall, the copy-protected CDs were still available in many states. Arik Hesseldahl, *Spitzer Gets*

Sony BMG roughly $6.5 million in return fees and manufacturing costs.[67] Although the twenty million MediaMax discs it distributed were never officially recalled,[68] Sony BMG ceased production of MediaMax discs in December of 2005.[69] Various state Attorneys General negotiated the destruction of the remaining stock of MediaMax CDs at Sony BMG's expense.[70] In addition, Sony BMG's subsequent settlement with the FTC established an incentive program to prompt retailers to return any remaining discs.[71]

Not surprisingly, Sony BMG artists and their management lashed out at the label for its use of these protection measures.[72] Even before news of the rootkit broke, artists expressed their frustration with protected CDs, which among other things, prevented fans from transferring music to their iPods.[73] In a message to fans, Tim Foreman, of Sony BMG band Switchfoot, wrote,

> We were horrified when we first heard about the new copy-protection policy that is being implemented by most major labels . . . and immediately looked into all of our options for removing this from our new album . . . . It is heartbreaking to see our blood, sweat, and tears over the past 2 years blurred by the confusion and frustration surrounding this new technology."[74]

This dissatisfaction only grew once artists and fans learned of the dangers posed by these technologies. The manager for Sony BMG artist Trey Anastasio, whose November 1 album release was marred by the inclusion

---

on Sony BMG's Case, BUS. WK., Nov. 29, 2005, http://businessweek.com/technology/content/nov2005/tc20051128_573560.htm.

67. Brian Garrity & Ed Christman, *supra* note 66.

68. Juan Carlos Perez, *FTC Seeks Public Comment on Sony Rootkit Settlement*, COMPUTER WORLD, Jan. 30, 2007, http://www.computerworld.com/action/article.do?command=viewArticleBasic&articleId=9009719&source=rss_news50.

69. Settlement Agreement at 27, *In re* Sony BMG CD Techs. Litig., No. 1:05-CV-09575 (S.D.N.Y. Dec. 28. 2005), *available at* http://www.eff.org/IP/DRM/Sony-BMG/sony_settlement.pdf.

70. Respondent Assurance of Voluntary Compliance or Discontinuance at 16, *In re* Sony BMG Music Entertainment (S.D.N.Y. Dec. 21, 2006), *available at* http://www.nj.gov/oag/newsreleases06/sony-bmg-agrmnt-12.21.06.pdf.

71. Press Release, Federal Trade Commission, Sony BMG Settles FTC Charges (Jan. 30, 2007), *available at* http://www.ftc.gov/opa/2007/01/sony.shtm.

72. Brian Hiatt, *Sony XCP Bomb Sparks Rage*, ROLLING STONE, Nov. 28, 2005, http://www.rollingstone.com/news/story/8878184/sony_xcp_bomb_sparks_rage.

73. Halderman & Felten, *supra* note 11, at 15.

74. Tim Rogers, *Stupid CD Copy Protection—Switchfoot Responds*, BLOGCRITICS MAGAZINE, Sept. 22, 2005, http://blogcritics.org/archives/2005/09/22/013800.php.

of XCP, called the incident "a complete fiasco that will impact the entire industry," and an "inexcusable blunder on the labels' part."[75] Another Sony BMG artist**,** My Morning Jacket, not only provided instructions on its website that enabled fans to bypass the MediaMax software on the band's album *Z*, but also sent over one hundred burned copies of the album to fans dissatisfied with the DRM.[76] In a New York Times Op-Ed, Damian Kulash, of the band OK Go, who narrowly avoided the inclusion of DRM on their EMI release *Oh No* in part because of the band's protestations, described copy protection software as "at best a nuisance, and at worst a security threat."[77]

The outcry from fans, artists, and consumer advocates alike gave rise to a palpable shift in the public perception of Sony BMG and its parent corporations.[78] Online petitioners called for a boycott of not only protected Sony BMG CDs, but Sony products generally.[79] In the fallout of the rootkit incident, one leading technology media outlet ranked Sony BMG's protected discs fifth in its list of the worst technology products in history.[80] The incident earned Sony BMG further distinction by being named one of the top ten "dumbest moments in business" for 2005.[81] Although the financial impact of this public relations disaster is difficult to estimate, Sony BMG remains, in the eyes of many consumers, inextricably associated with its misguided attempts at content protection.

B. Externalities Arising from the Rootkit Incident

Aside from its impact on Sony BMG and its customers, the rootkit incident inflicted broadly dispersed costs on individuals and institutions oth-

---

75. Hiatt, *supra* note 72.

76. James Montgomery, *My Morning Jacket Tackle Copy-Protection Software Problems—By Burning CDs For Fans*, MTV.com, Dec. 16, 2005, http://www.mtv.com/news/articles/1518240/20051215/%20my_morning_jacket.jhtm.

77. Damian Kulash Jr., *Buy, Play, Trade, Repeat*, N.Y. TIMES, Dec. 6, 2005, at A27.

78. Olga Kharif, *For Sony, a Pain in the Image*, BUS. WK., Dec. 2, 2005, http://www.businessweek.com/technology/content/dec2005/tc20051202_241333.htm; *Sony BMG Hits the Wrong Note*, COMPUTER BUS. REV. ONLINE, Nov. 16, 2005, http://www.cbronline.com/article_feature.asp?guid=44AF133B-9126-4207-A80C-60286AFAB943.

79. The Sony Boycott Blog, http://www.boycottsony.us/ (last visited Sept. 6, 2007); Boycott Sony!!! Petition, PetitionOnline.com, http://www.petitiononline.com/bcsony/petition.html (last visited Sept. 6, 2007).

80. Dan Tynan, *The 25 Worst Tech Products of All Time*, PC WORLD, May 26, 2006, http://www.pcworld.com/article/id,125772-page,2/article.html.

81. Adam Horowitz et al., *101 Dumbest Moments in Business*, BUSINESS 2.0, Jan. 2006, at 98, *available at* http://money.cnn.com/magazines/business2/101dumbest/2006.

erwise unconnected to Sony BMG's DRM strategy. First, the insecurity introduced into individual computers led to network-wide vulnerabilities. Second, the rootkit incident undermined consumer acceptance of digital rights management technology. The first of these externalities foisted the costs of network insecurity onto the public, while the second decreased the value and viability of DRM strategies and forced Sony BMG's partners and competitors within the content protection industry to rethink their practices.[82]

Because of the distributed nature of the information infrastructure, overall network security is, in part, a function of the security of the millions of private and personal computers that comprise it.[83] As a result, attacks on individual computers endanger, by extension, the network itself. Improving and maintaining the security of our collective information infrastructure is an established national priority[84]—a national priority directly threatened by Sony BMG's DRM.

These network vulnerabilities could manifest themselves in a number of ways. First, XCP-infected machines could be exploited by attackers to penetrate otherwise secure corporate, university, government, or military networks. In the weeks following the public announcement of the rootkit, the number of networks containing at least one installation of XCP topped half a million.[85] These networks suffered an increased risk of attack, leaving the sensitive data they stored subject to theft or tampering.

Second, computers infected with Sony BMG's DRM could serve as launching points for attacks on third party machines. An attacker could utilize the vulnerabilities created by these DRM systems to enlist thou-

---

82. While network insecurity almost certainly functions as a negative externality, the impact of the lessened value of DRM is more difficult to classify in terms of overall social utility.

83. *See* JAMES ELLIS ET AL., SOFTWARE ENG'G INST., REPORT TO THE PRESIDENT'S COMMISSION ON CRITICAL INFRASTRUCTURE PROTECTION (1997), http://www.cert.org/pres_comm/cert.rpcci.body.html.

84. *See, e.g.*, CRITICAL INFORMATION INFRASTRUCTURE PROTECTION AND THE LAW: AN OVERVIEW OF KEY ISSUES (Stewart D. Personick & Cynthia A. Patterson eds., National Academies Press 2003); PRESIDENT'S CRITICAL INFRASTRUCTURE PROT. BD., THE NATIONAL STRATEGY TO SECURE CYBERSPACE (2003), *available at* http://www.whitehouse.gov/pcipb/cyberspace_ strategy.pdf.

85. Quinn Norton, *Sony Numbers Add Up to Trouble*, WIRED, Nov. 15, 2005, http://wired-vig.wired.com/politics/security/news/2005/11/69573; Dan Kaminsky, *Welcome To Planet Sony*, DOXPARA RESEARCH, Nov. 15, 2005, http://www.doxpara.com/?q=/node/1129.

sands of machines, unbeknownst to their owners, into massive botnets[86]—armies of so called "zombie" computers—which are directed to relay spam or conduct crippling distributed denial of service (DDOS) attacks.[87] Past DDOS targets have included corporations and national security assets, including the infrastructure of the internet itself.[88] Zombies may also be used to relay anonymous messages and hide the activities and communications of criminal and terrorist organizations from law enforcement.[89]

Whether through direct access to protected networks or through distributed attacks, Sony BMG's DRM threatened the basic operation of critical services that rely on the network infrastructure, among them, financial, communications, and disaster response services. The worst-case scenarios of rootkit-enabled attacks were nothing short of catastrophic. Although these potential outcomes may smack of doomsday prognostication, the Department of Homeland Security took note of the public threat posed by Sony BMG's DRM, cautioning that the XCP rootkit or similarly misguided attempts to control copyrighted works could interfere with the response to public health crises by compromising the security of the information infrastructure.[90]

---

86. Posting of Ed Felten to Freedom to Tinker, http://www.freedom-to-tinker.com/?p=1150 (Apr. 26, 2007, 10:41 EST) (discussing botnet threats in general).

87. A distributed denial of service attack occurs when multiple compromised systems flood the bandwidth or resources of a targeted system, usually one or more web servers. *See, e.g.*, Press Release, U.S. Department of Justice, Man Pleads Guilty to Infecting Thousands of Computers Using Worm Program then Launching them in Denial of Service Attacks (Dec. 28, 2005), *available at* http://www.cybercrime.gov/clarkPlea.htm; Ellen Messmer, *Web Sites Unite to Fight Denial-of-Service War*, NETWORK WORLD, Sept. 25, 2000, http://www.networkworld.com/news/2000/0925userdefense.html?nf&_ref=858966935; Jaikumar Vijayan, *VeriSign Details Massive Denial-of-Service Attacks*, COMPUTER WORLD, Mar. 16, 2006, http://www.computerworld.com/developmenttopics/websitemgmt/story/0,10801,109631,00.html.

88. *See, e.g.*, Tim Weber, *Criminals 'may overwhelm the web'*, BBC NEWS, Jan. 25, 2007, http://news.bbc.co.uk/2/hi/business/6298641.stm; John Leyden, *Telenor Takes Down 'massive' Botnet*, THE REGISTER, Sept. 9, 2004, http://www.theregister.co.uk/2004/09/09/telenor_botnet_dismantled/; Gregg Keizer, *Dutch Botnet Suspects Ran 1.5 Million Machines*, TECHWEB TECH. NEWS, Oct. 21, 2005, http://www.techweb.com/wire/security/172303160.

89. Comment of Edward W. Felten & J. Alex Halderman to the United States Copyright Office, concerning RM 2005-11—Exemption to Prohibition on Circumvention of Copyright Protection Systems for Access Control Technologies (Dec. 1, 2005), *available at* http://www.copyright.gov/1201/2006/comments/mulligan_felten.pdf.

90. *Homeland Security Warns Against Anti-Piracy*, WASHINGTONPOST.COM, Nov. 11, 2005, http://www.washingtonpost.com/wp-dyn/content/video/2005/11/11/VI2005111101160.html. Stewart Baker, assistant secretary of policy at the Department of Home-

Aside from the social cost of decreased security of the information infrastructure, the rootkit incident resulted in a second externality. By dramatically increasing public awareness of the restrictions on access and copying imposed by DRM technologies, while simultaneously corroding consumer confidence in their safety, the rootkit incident likely undermined the significant investments of both content providers and protection measure vendors in such technology. In the wake of the rootkit fiasco, major labels abandoned the use of DRM on CDs,[91] and leading protection measure vendors ceased development of new CD-based DRM systems.[92] But unlike the collective costs to security imposed by the rootkit incident, the reduced viability of DRM in the consumer music market may well represent a positive externality, rather than a negative one. To the extent the constraints and risk DRM imposed on consumers outweighed any benefits they conferred on copyright owners and the public, the reduction of DRM in the consumer marketplace could increase overall utility.

The impact of the rootkit incident has extended beyond the CD market, coloring consumer perception of the desirability of DRM and forcing copyright owners and technology companies to rethink their content protection strategies. DRM, of course, faced criticism long before the rootkit

---

land Security, warned copyright holders against overly aggressive efforts to protect copyrighted material:

> I wanted to raise one point of caution as we go forward, because we are also responsible for maintaining the security of the information infrastructure of the United States and making sure peoples' [and] businesses' computers are secure. . . . There's been a lot of publicity recently about tactics used in pursuing protection for . . . CDs in which questions have been raised about whether the protection measures install hidden files on peoples' computers that even the system administrators can't find. It's very important to remember that it's your intellectual property; it's not your computer. And in the 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.

Id.; Brian Krebs, *DHS Official Weighs In on Sony*, WASHINGTONPOST.COM, Nov. 11, 2005, http://blog.washingtonpost.com/securityfix/2005/11/dhs_official_weighs_in_on_sony.html.

91. Robert Thompson & Tom Ferguson, *Copy-Protection Curtailed*, BILLBOARD, Dec. 16, 2006, at 27 ("EMI Music Group has dropped copy-protection technology from new CD releases internationally amid concerns it was not slowing piracy. The decision means that no major labels are currently releasing copy-protected discs.").

92. *Macrovision Scraps CD Protection Software, Readies New Download Service*, CONSUMER ELECTRONICS DAILY, Feb. 23, 2007 ("[Macrovision CEO Fred] Amoroso conceded that the discovery in late 2005 of a rootkit in Sony BMG CDs containing First4Internet's copy protection software 'spooked the industry.'").

incident.[93] But after the general public became more attuned to the presence and effects of DRM, in part through the debate sparked by the XCP rootkit, these criticisms came from not only consumer advocates, but from leading technology companies with intimate ties to the music industry as well. In December of 2005, Bill Gates decried the lack of "simplicity and interoperability" of the DRM technologies protecting music downloads.[94] Others like Yahoo! Music chief David Goldberg urged the industry to drop DRM on downloads.[95] These early critiques of DRM led the music industry to implement limited experiments in legitimate DRM-free downloads.[96]

These experimental DRM-free releases gave way to calls for more fundamental changes. In February of 2007, Apple CEO Steve Jobs published an open letter in which he called for the major record labels to "abolish DRM[] entirely."[97] Less than a month later, EMI and Apple announced that EMI's entire digital catalog would be available without DRM on iTunes and through other retailers.[98] During the joint Apple/EMI

93. *See, e.g.*, Pamela Samuelson, *Intellectual Property and the Digital Economy: Why the Anti-Circumvention Regulations Need to be Revised*, 14 BERKELEY TECH. L.J. 519, 556 (1999).

94. *Gates: Digital Locks Too Complex*, BBC NEWS, Dec. 15, 2006, http://news.bbc.co.uk/1/hi/technology/6182657.stm; Michael Arrington, *Bill Gates On The Future Of DRM*, TECHCRUNCH, Dec. 14, 2006, http://www.techcrunch.com/2006/ 12/14/bill-gates-on-the-future-of-drm/.

95. Ian C. Rogers, *Dave Goldberg to Record Labels: No DRM, Please*, YAHOO! MUSIC BLOG, Feb. 25, 2006, http://ymusicblog.com/blog/2006/02/25/dave-goldberg-to-record-labels-no-drm-please/; John Borland, *Yahoo Exec: Labels Should Sell Music Without DRM*, CNET NEWS.COM, Feb. 23, 2006, http://news.com.com/8301-10784_3-6042756-7.html?part=rss&tag=6042756&subj=news.

96. Jessica Simpson, Jesse McCartney, and Lily Allen were among the artists included in these initial trials for DRM-free downloads. Ian C. Rogers, *Buy A Customized MP3 At Yahoo! Music*, YAHOO! MUSIC BLOG, July 19, 2006, http://ymusicblog.com/blog/2006/07/19/buy-a-customized-jessica-simpson-mp3-at-yahoo-music/; *Is EMI Experimenting With MP3's?*, HYPEBOT, Nov. 29, 2006, http://hypebot.typepad.com/hypebot/2006/11/is_emi_experime.html; Ben Fritz, *Yahoo Tests 'Right' to MP3 Downloads*, VARIETY.COM, Sept. 18, 2006, http://www.variety.com/article/VR1117950324.html?categoryid=1009&cs=1&nid=2570.

97. STEVE JOBS, THOUGHTS ON MUSIC (2007), http://www.apple.com/hotnews/thoughtsonmusic/.

98. Press Release, EMI, EMI Music Launches DRM-free Superior Sound Quality Downloads Across its Entire Digital Repertoire (Apr. 2, 2007), *available at* http://www.emigroup.com/Press/2007/press18.htm; Press Release, Apple, Apple Unveils Higher Quality DRM-Free Music on the iTunes Store (Apr. 2, 2007), *available at* http://www.apple.com/pr/library/2007/04/02itunes.html. The first DRM-free EMI release, the album

press conference, Jobs noted the rootkit as an example of the failure of CD-based DRM.[99] Other digital music retailers, including Microsoft, followed suit and agreed to provide DRM-free EMI music.[100]

Obviously, the fear of rootkit-like security vulnerabilities was not the sole, or even primary, impetus for this shift in the market for digital music downloads. But the rootkit incident contributed to the creation of an environment amenable to this change in the prevailing wisdom among record labels and their online content distributors. The rootkit incident thrust the negative implications of DRM into the public consciousness on a broader scope than had previous rounds of criticism. These implications included not only the privacy and security interests directly at stake in the rootkit incident, but also more general concerns over restrictions on noninfringing uses, portability, and platform independence. As a validation of the long-standing and frequently marginalized critiques of DRM, the rootkit incident made it more difficult for these criticisms to be dismissed out of hand. If the rest of the music industry follows EMI in its march away from DRM, the rootkit incident may prove, in retrospect, to have been a major strategic turning point.

But even copyright holders that continue to insist upon DRM recognize its public relations pitfalls in the current marketplace. In a transparent effort to divert attention away from the restrictions placed on users by technological protection measures, some have called for a shift in terminology, dropping "Digital Rights Management"—a term once thought consumer-friendly—and replacing it with the euphemistic "Digital Con-

---

The Good, The Bad & The Queen, by the innominate EMI band, was made available immediately. The remainder of the EMI catalog was scheduled for DRM-free release on iTunes in May of 2007.

99. Eric Nicoli, CEO, EMI Group & Steve Jobs, CEO, Apple, Q&A at EMI Press Conference (Apr. 2, 2007), *audio available at* http://w3.cantos.com/07/pjxrobbi-703-5zvx0/interviews.php?task=view; *Jobs Talks New iTunes Functions, DRM and Video, iPod Storage*, APPLEINSIDER, Apr. 2, 2007, http://www.appleinsider.com/articles/07/04/02/jobs_talks_new_itunes_functions_drm_and_video_ipod_storage_transcript.html. Apple's position was likely influenced, at least in part, by growing international opposition to its iTunes DRM. See Apple DRM illegal in Norway: Ombudsman, The Register, http://www.theregister.co.uk/2007/01/24/apple_drm_illegal_in_norway/?TB_iframe=true&height=650&width=950 (Jan. 24, 2007); Thomas Crampton, iTunes legal attacks spread from France, International Herald Tribune, http://www.iht.com/articles/2006/06/08/business/apple.php (June 9, 2006).

100. *See, e.g.*, Elizabeth Montalbano, *Microsoft Will Sell DRM-free Songs*, PC WORLD, Apr. 6, 2007, http://www.pcworld.com/article/id,130472/article.html.

sumer Enablement."[101] Whether substantive changes in current business models prevail or the industry instead adopts cosmetic fixes, the market for DRM has undergone an important shift, in part as the result of the rootkit incident.

The harms that resulted from the rootkit incident affected all parties to the sale and licensing of protected Sony BMG CDs. Customers received a product tainted by reduced functionality, undisclosed invasions of privacy, and increased vulnerability to security breaches. Sony BMG and its artists hardly benefited from this deal, suffering both financial and reputational repercussions. The externalities that flowed from the rootkit incident undermined collective investments in network security and DRM technology for parties entirely removed from Sony BMG and its ill-designed protection measures. In the end, it appears safe to conclude that no one's best interest—especially not that of Sony BMG—was served by the distribution of XCP and MediaMax. The next Part attempts to surmise what market considerations could have convinced Sony BMG that the distribution of these protection measures was a reasonable, self-interested decision.

III. MARKET INFLUENCES

Failures of software developers to adequately safeguard the security of their users' systems and information come as no shock to those familiar with the state of computer security. The values and incentives that give rise to these failures are well documented.[102] Users frequently undervalue their own privacy and security,[103] and even those who claim to place a high value on these interests often act inconsistently with those values.[104] Because increased security provides little or no competitive advantage through product differentiation, firms recognize that the significant investments in time and resources needed to identify and eliminate the bugs that create insecurity will not be recouped.[105] As a result, firms systematically under-invest in software security and fail to eliminate vulnerabilities.

---

101. Glen Dickson, *NCTA: HBO's Zitter Says DRM Is Misnomer*, BROADCASTING & CABLE, May 9, 2007, http://www.broadcastingcable.com/article/CA6440876.html.

102. *See* Ross Anderson & Tyler Moore, *The Economics of Information Security*, 314 SCIENCE 610 (2006), *available at* http://www.cl.cam.ac.uk/~twm29/science-econ.pdf.

103. *See* Alessandro Acquisti & Jens Grossklags, *Privacy and Rationality in Individual Decision Making*, IEEE SECURITY & PRIVACY, Jan.-Feb. 2005, at 26.

104. *See id.*

105. *See* Bill Thompson, *Taking Computer Insecurity Seriously*, BBC NEWS, Sept. 17, 2004, http://news.bbc.co.uk/2/low/technology/3666702.stm; Jeordan Legon, *As Net Attack Eases, Blame Game Surges*, CNN.COM, Jan. 28, 2003, http://www.cnn.com/2003/

However, these incentives to under-invest in security cannot fully explain the Sony BMG rootkit incident. Typically, software vulnerabilities result from a developer's failure to remove incidental and unintended infirmities in its code. But the rootkit incident in large part resulted from the *intentional* introduction of components and functionality that undermined user security and privacy in the service of content protection.[106] From the perspective of protection measure developers and content owners, these security and privacy flaws served as features rather than bugs.[107] In this sense, the motivations underlying the rootkit incident share some common features with those that spur the development of spyware. Because it differs so fundamentally from the longstanding understanding of how insecure software makes its way to market, the Sony BMG rootkit incident raises new questions about the incentives to protect or subvert user security and privacy in the context of DRM technology.

This Part examines two basic sets of market-based explanations of Sony BMG's decision-making process. The first considers possible failures to grasp the likely impact of its technology, and suggests systematic inadequacies in Sony BMG's review of the DRM systems it licenses. The second countenances more informed and, consequently, more deliberate cost-benefit calculations that could encourage the use of cloaking technologies and inadequate disclosures. Ultimately, although we conclude that this second set of explanations is the more plausible, both likely contributed, to varying degrees, to the release of these protection measures.

A. The Rootkit Incident as Mistake

Imperfect information and bounded rationality offer perhaps the most charitable explanations of Sony BMG's decision to distribute XCP and MediaMax. Given the resources and sophistication of Sony BMG, this ex-

---

TECH/internet/01/27/worm.why/; Brendan I. Koerner, *Ain't No Network Strong Enough*, SALON.COM, Aug. 31, 2000, http://archive.salon.com/tech/review/2000/08/31/schneier/; Mindy Blodgett, *Is Your Business as Safe as You Think?*, CNN.COM, July 16, 1999, http://www.cnn.com/TECH/computing/9907/16/security-ent.idg/index.html.

106. Some of the risks created as a result of the rootkit incident were the result of failures to eliminate bugs rather than the intentional introduction of risk. This more traditional narrative, for example, explains the flaws in the uninstaller tools and patches released after the disclosure of the harms of XCP and MediaMax. MediaMax's privilege escalation vulnerability likewise can be explained without implying any harmful intent on the part of its developers.

107. As Professor Felten has explained, these vulnerabilities are "caused not by any flaws in [the] execution of their copy protection plan, but from the nature of the plan itself." Posting of Ed Felten to Freedom to Tinker, http://www.freedom-to-tinker.com/?p=934 (Nov. 22, 2005, 03:51 EST).

planation seems at best incomplete. But even if Sony BMG lacked critical information about the dangers posed by its protection measures or miscalculated their likelihood and severity, its decision points to a culpable failure of internal procedures to safeguard against the wide-scale distribution of flawed protection measures.

A good-faith mistake on the part of Sony BMG could have arisen in two ways. First, Sony BMG could have been unaware of the objectionable features of its DRM—at least those not directly related to the constraints placed on accessing and copying music. Second, Sony BMG could have been misinformed or misled about the dangers posed by the various components of its protection measures.

Both of these explanations depend on a lack of adequate pre-release security reviews of protection measures. Sony BMG has offered no public indication that any pre-release security review occurred. Assuming Sony BMG did not intentionally distribute software with knowledge of the dangers it posed, any such review must have failed to identify the threats inherent in XCP and MediaMax. It is unlikely that Sony BMG lacked sufficient in-house security expertise to meaningfully examine the functionality of the protection measures it licensed. Given that Sony Corporation of America, whose holdings include Sony Electronics and Sony Computer Entertainment America, controls a 50% interest in Sony BMG, more than adequate technical analysis was within reach. Moreover, external security review of new DRM schemes is common within the music industry. And as demonstrated by the research of F-Secure[108] and Mark Russinovich,[109] as well as by the analysis of Ed Felten and J. Alex Halderman,[110] trained security professionals could have easily identified the security risks posed by these protection measures.

Aside from a disregard for user security,[111] another explanation for the lack of meaningful security review is overconfidence in the protection measure vendors who provided these technologies. In retrospect, any such confidence was obviously misplaced. But even without the benefit of hindsight, Sony BMG had good reason to subject its vendors' products to scrutiny. Prior to inking the deal to provide XCP to Sony BMG, First4Internet's business focused on content filtering, particularly the

108. *See* Hamm, *supra* note 13.

109. *See* Mark's Blog, *supra* note 8 (Oct. 31, 2005, 11:04 PST).

110. *See* Halderman & Felten, *supra* note 11.

111. As discussed *infra* in Section III.B, an undervaluing of user security and privacy could explain Sony BMG's decision.

automated recognition of pornographic images.[112] Aside from an earlier revision on XCP used by a number of labels on a smattering of pre-release CDs,[113] First4Internet had no apparent expertise or experience in content protection software.

SunnComm, the company that delivered MediaMax, offered even more cause for concern. The company began as a provider of Elvis impersonation services.[114] After a change in management following a false press release announcing a non-existent $25 million production deal with Warner Brothers,[115] the company purchased a 3.5" floppy disk factory in 2001, displaying a disturbing dearth of technological savvy.[116] After two employees announced their intention to leave the fledgling company to develop copy protection software, SunnComm convinced the pair to lead a new division, leaving both Elvis and floppy discs behind in order to develop what would become MediaMax.[117]

Sony BMG—perhaps realizing too late its misplaced trust in SunnComm, or perhaps simply hoping to recoup some of its financial and public relations losses—filed a lawsuit against the Amergence Group (a re-branded SunnComm)[118] in July of 2007. Sony BMG's claims include

---

112. *See First 4 Internet Powers New Anti-Porn Solutions at Europe's Biggest Security Show; Major New Products from PixAlert, Pure Content and Green Technology Meet Growing Corporate Need to Filter Pornography*, TMCNET, Apr. 20, 2005, http://www.tmcnet.com/usubmit/2005/apr/1136356.htm. After the rootkit incident, First4Internet continued to do business under the name Fortium Technologies. *See* Robert Lemos, *Sony BMG Sues Copy-protection Maker*, SECURITYFOCUS, July 13, 2007, http://www.securityfocus.com/brief/547.

113. *See* Sion Barry, *Controlling Illicit Internet Content Drives F4I Success*, ICWALES, June 15, 2005, http://icwales.icnetwork.co.uk/0300business/0100news/tm_objectid=15631868&method=full&siteid=50082-name_page.html.

114. Ashlee Vance, *Is SunnComm a Sham or the Next, Big DRM Success?*, THE REGISTER, Sept. 27, 2004, http://www.theregister.co.uk/2004/09/27/sunncomm_death_or_glorry/print.html.

115. Complaint for Injunctive and Other Relief, U.S. Sec. and Exch. Comm'n v. Paloma (D.D.C. Apr. 11, 2002), *available at* http://www.sec.gov/litigation/complaints/complr17462.htm.

116. SunnComm purchased the floppy drive company, which was formerly a failed oil and gas company, in part to avoid SEC scrutiny by merging with a fully reporting company. *See* Vance, *supra* note 114.

117. *Id.*

118. SunnComm, too, underwent something of a re-branding after the rootkit incident, rechristening itself the Amergence Group. Press Release, The Amergence Group, SunnComm Establishes New Subsidiary—The Amergence Group (Jan. 26, 2007), *available at* http://www.amergencegroup.com/news/amergingnews.asp?grammid=200701261030.

negligence and breach of contract, alleging that MediaMax was defective and failed to satisfy SunnComm's warranty.[119] The Amergence Group contends that Sony BMG retained "final authority" over the functional specifications of MediaMax, and that SunnComm simply delivered the product demanded by Sony BMG.[120] This litigation, as it proceeds, may well reveal the extent of Sony BMG's knowledge of the objectionable features of its DRM.

Until such information is available, Sony BMG's sophistication[121] and access to both internal and external resources offer good reasons to question the likelihood that it was in the dark as to the existence of the dangers posed by the rootkit and the other objectionable features of XCP and MediaMax. Even assuming Sony BMG was oblivious as to the details of its DRM, the failure to act expeditiously once notified by F-Secure of the rootkit and its dangers suggests that a lack of knowledge alone fails to fully explain Sony BMG's actions. In any case, to the extent that ignorance of the functionality and likely effects of its DRM influenced Sony BMG's decision-making, its failure to independently review these technologies evinces an undervaluation of the documented potential effects of DRM on user security and privacy.

B. The Rootkit Incident as Calculated Risk

Since characterizations of the rootkit incident as the result of a good-faith mistake by Sony BMG fail to fully account for its internal decision-making, explanations that presume some degree of knowledge present more plausible scenarios. Understanding why Sony BMG would knowingly distribute protection measures that carried the risks associated with XCP and MediaMax requires consideration of the relative value propositions presented by CD-based DRM to content owners and customers. Although DRM, in theory, offers copyright holders some benefit from reduced copying, consumers generally see DRM as a poor bargain since it requires them to pay the same price for a product with diminished func-

---

119. *See* Summons Notice, Sony BMG Entm't v. Amergence Group, No. 602201-2007 (N.Y. Sup. Ct.) (on file with authors).

120. Press Release, The Amergence Group, Sony-BMG Files Suit Against Amergence Group (July 11, 2007), *available at* http://www.marketwire.com/mw/release.do?id=750315.

121. Sony, along with Philips, owns the rights to the core DRM patents of Intertrust. In theory, at least, Sony BMG could have implemented a suite of better technical solutions. *See* Press Release, Sony Corporation of America, Philips and Sony Lead Acquisition of Intertrust, *available at* http://www.sony.com/SCA/press/021113.shtml (Nov. 13, 2002).

tionality. Underhanded tactics such as those used by Sony BMG offer one way to overcome this skepticism, although this story should counsel against their future use.

Although the precise amounts are uncertain, the music industry loses revenues each year as a result of copyright infringement.[122] Songs copied on peer-to-peer networks, BitTorrent, and other lesser-known corners of the darknet contribute to these losses, as does large-scale CD piracy and the casual physical copying of CDs by everyday consumers.[123] DRM is intended to serve as a partial solution to the widespread infringement of music industry copyrights, but, as the industry is likely aware, CD-based DRM cannot hope to address two of these three sources of infringement. Since only a single unrestricted copy of a particular track is necessary to rapidly populate peer-to-peer and other networked methods of file transfer, measures like XCP and MediaMax are all but worthless when it comes to preventing infringement on the internet.[124] And protection measures that can be easily thwarted[125] pose no genuine hurdles for the sophisticated, large-scale commercial pirates that press upwards of one billion counterfeit CDs each year.[126]

The value of CD-based DRM like XCP and MediaMax, therefore, flows from its ability to prevent the casual schoolyard trading of burned CDs and other varieties of personal copying. The precise scope of financial harm caused by such purported infringement is unclear.[127] Nor does

---

122. RIAA, Piracy: Online and on the Street, http://www.riaa.com/physicalpiracy.php?content_selector=piracy_details_online (last visited July 30, 2007).

123. *Id. See also* Peter Biddle & Paul England, *The Darknet and the Future of Content Distribution*, ACM SIGCOMM COMPUTER COMM. REV., Oct. 2001, at 140, *available at* http://msl1.mit.edu/ESD10/docs/darknet5.pdf (describing the darknet as "a collection of networks and technologies used to share digital content [and] an application and protocol layer riding on existing networks" and citing as examples of darknets "peer-to-peer file sharing, CD and DVD copying, and key or password sharing on email and newsgroups.").

124. *See* Halderman & Felten, *supra* note 11, at 2.

125. As discussed *infra* in the text accompanying note 179, MediaMax can be defeated by simply holding down a computer's shift key. Earlier DRM systems could be circumvented using just adhesive tape or a felt tip pen. HALDERMAN, *supra* note 4, at 4, 5.

126. *Pirate CD Sales Top 1 Billion*, CNN.COM, July 10, 2003, http://edition.cnn.com/2003/BUSINESS/07/10/music.piracy/; *Pirate CD Sales Hit Record High*, BBC NEWS, July 22, 2004, http://news.bbc.co.uk/2/hi/entertainment/3916681.stm.

127. Industry research indicates that such "social sharing" accounts for as much as 37% of music acquisition by volume. NPD GROUP, NARM/NPD 2007, PHASE ONE, CONSUMERS & MUSIC DISCOVERY 4 (2007), *available at* http://www.digitalmusicnews.com/research/npd_presentation_narm. However, as with earlier projections of harm aris-

any available evidence reveal the effectiveness of these measures in limiting such activity. Perhaps in recognition of the tenuous argument for the utility of these measures, even on this single front of the war against infringement, the music industry is quick to downplay its expectations for CD-based DRM, typically referring to these protection measures as mere "speed bumps" or inconveniences intended to keep honest customers honest.[128] But given their rudimentary design, these protection measures disproportionately affect those customers with the least knowledge of the operations of their computers, precisely those reasonably expected to pose the least threat of infringement. From the content owners' own perspective, these protection measures offer only marginal value, and even this valuation may be the result of overestimates of the effectiveness of CD-based DRM.

If the value of CD-based DRM to content owners is low, albeit positive, the value of these protection measures to customers is almost unquestionably negative. Even at the time of the rootkit incident, the overwhelming majority of CDs were sold without DRM;[129] customers were, as a technological matter, free to copy songs from these discs to their hard drives, transfer them to iPods, burn them to CDs, and listen to them using the software of their choice.[130] XCP and MediaMax altered long-standing consumer expectations[131] by placing technological and contractual limits on customers' ability to use their CDs in the manner to which they were accustomed.

---

ing from peer-to-peer downloads, estimates of the relative proportion of these burned and ripped copies that translate to lost sales would likely vary significantly.

128. Sony spokesman Nathaniel Brown characterized SunnComm's first copy protection scheme in the following manner after J. Alex Halderman reported that it was easily disabled: "Copy management is intended as a speed bump, intended to thwart the casual listener from mass burning and uploading. We made a conscious decision to err on the side of playability and flexibility." John Borland, *Shift Key Breaks CD Copy Locks*, CNET NEWS.COM, Oct, 7, 2003, http://news.com.com/2100-1025_3-5087875.html.

129. In 2005, over 600 million CDs were sold in the United States. *See US CD Album Sales Show 7% Slide*, BBC NEWS, Dec. 29, 2005, http://news.bbc.co.uk/2/hi/entertainment/4566186.stm. Of those, the millions of CDs protected by XCP and MediaMax represented only a small percentage.

130. *See infra* notes 132-136.

131. Consumer expectations flow from prior experience with similar objects and information. These experiences are in turn a result of the capacity of the technology, laws, norms, and markets. Consumer expectations of interacting with DVDs today reveals how these forces can come together in ways that create expectations different from those which prevailed during the CD era.

Empirical research has cataloged the deep-seated expectations of consumers with respect to their interaction with digital music. In a study conducted in the European Union, consumers indicated uniform and strong beliefs in their right to move digital music between devices.[132] Similarly, individuals shared a strong conviction that copying for their own purposes is legal,[133] and a high percentage of the survey population had burned their own music mixes in the prior six months.[134] While survey participants' belief in the legality of "sharing" music was less strong and consistent,[135] they reported a significant amount of sharing with family and friends.[136]

These consumer expectations are firmly rooted in the pre-digital patterns of consumption and use of recorded music. Concerns over private copying enabled by new technologies are, of course, nothing new. Nearly every advance in the recording and distribution of music has sparked near hysteria from then-dominant rights holders. Music publishers balked at the player piano,[137] the phonograph[138] and radio of both the terrestrial[139] and internet[140] varieties. And long before the music industry feared peer-to-peer infringement, reel-to-reel copying led the industry to infamously proclaim that "Home Taping is Killing Music."[141] The concerns that motivate

---

132. According to the study, 81% of those surveyed thought it legal to play a purchased file on different devices. NICOLE DUFFT ET AL., INDICARE, DIGITAL MUSIC USAGE AND DRM: RESULTS FROM AN EUROPEAN CONSUMER SURVEY 42 (2005), *available at* http://www.indicare.org/tiki-download_file.php?fileId=110.

133. In the study, 73% of users surveyed thought it was legal to make a copy of a CD or file which they had bought for themselves, for their own use. *Id.*

134. Of all digital music users surveyed, 80% had burned their own mixes to CD over the past 6 months, 39% had done so several times per month or more often. The share of teens that burn their own CDs several times per month or more often is 46%, compared to 34% of the 40+ group. *Id.* at 16. In Germany, almost 90% of the digital music users like to burn their own mixes on CD compared to "only" 75% in the UK. *Id.* at 18 tbl. 3.2.

135. *Id.* at 42.

136. More than three quarters of digital music users have shared music files with their family members and friends over the past 6 months; 60% have shared music files with other people. Again, teens are the most active music file sharers; about half of them share music files with friends and family several times per month or more often.
Id. at 16.

137. LAWRENCE LESSIG, FREE CULTURE: HOW BIG MEDIA USES TECHNOLOGY AND THE LAW TO LOCK DOWN CULTURE AND CONTROL CREATIVITY 55-56 (2004), *available at* http://www. jus.uio.no/sisu/free_culture.lawrence_lessig/portrait.pdf.

138. *Id.*

139. *See id.* at 58-59.

140. *See id.* at 195-99.

141. Neil Strauss, *THE POP LIFE; 2 Big Forces Converging To Change the Sale of Music*, N.Y. TIMES, Dec. 10, 1998, at E1.

DRM are simply a continuation of this pattern of hostility to disruptive technologies.

Although engineering constraints have historically limited the copying of music, digital works are trivially copied without any loss of quality. In part driven by the lack of practical constraints on digital copying, DRM proactively introduces technological hurdles that exceed those available to earlier generations of copyright holders, displacing the traditionally porous enforcement of copyright with limits embedded in and enforced by software code.[142] In contrast, previous mechanisms for addressing infringement intruded less far less on the consumer's experience of the purchased music. For example, the Serial Copy Management System, which controlled downstream copying of the ill-fated Digital Audio Tape format, did not impede the use of the original tape or even the recording of first-generation copies.[143] DRM, on the other hand, frequently constrains the portability of music by tethering it to particular devices or platforms. Consumers are limited in their ability to experience the music on their own terms, in the time, place, and even sequence of their choice. Their ability to copy, share, and recode content is likewise constrained in a manner that offends many users' perceptions of fairness, if not law.

The constraints imposed by DRM generally reduce the value to consumers of protected content. Information goods typically increase in value as the number and extent of their possible uses increase.[144] With respect to DRM, consumers will, in principle, pay more for goods with liberal usage rules. In addition, more consumers can be expected to purchase such goods.[145] Consumers regard media with very limited uses as the equivalent of damaged goods[146] and will pay less for them, if they are willing to purchase them at all.[147] In short, CD-based DRM renders the protected discs

142. *See* Radin, Margaret Jane, *Regulation by Contract, Regulation by Machine*, 160 J. Inst. & Theoretical Econ. 142, 151-153 (2004); *see generally* LAWRENCE LESSIG, CODE AND OTHER LAWS OF CYBERSPACE (1999).

143. *See* Digital Audio Recording Devices and Media Act of 1992, 17 U.S.C. §§ 1001-1010 (2000).

144. CARL SHAPIRO & HAL R. VARIAN, INFORMATION RULES: A STRATEGIC GUIDE TO THE NETWORK ECONOMY 97-102 (1998).

145. This principle is borne out by the INDICARE survey results, which indicate that people are willing to pay substantially more for digital music with more functionality. *See* DUFFT ET AL., *supra* note 132, at 25.

146. *See* SHAPIRO & VARIAN, *supra* note 144.

147. *See* NATALI HELBERGER ET AL., FIRST UPDATE OF THE STATE-OF-THE-ART REPORT: DIGITAL RIGHTS MANAGEMENT AND CONSUMER ACCEPTABILITY: A MULTI-DISCIPLINARY DISCUSSION OF CONSUMER CONCERNS AND EXPECTATIONS 33-34 (2005), *available at* http://www.indicare.org/tiki-download_file.php?fileId=111.

less valuable to consumers. Yet this reduction in functionality is not counterbalanced by any proportionate decrease in cost. DRM-protected CDs are sold at roughly the same price as standard non-protected CDs.[148] Some protected CDs include bonus features like music videos or interactive artist biographies, but for most consumers these features were likely insufficient to compensate for the reduction in basic functionality of the protected discs.

Another factor in choosing to surreptitiously deploy DRM, beyond skirting consumer resentment, was that Sony BMG likely underestimated the public reaction to the security and privacy threats created by its DRM. Both research and market history have demonstrated that many users are willing to trade security and privacy for ease of use, desired functionality, or even small sums of money.[149] These results could lead a firm to place minimal value on user security and privacy in its risk calculus. In the rootkit incident, these assumptions proved incorrect. Consumers, it would appear, care enough about privacy and security to want to make the decision about when and whether to trade it away for themselves. In part, the strong reaction to these faulty protection measures could stem from deeply ingrained expectations about our experience of music. In contrast to browsing the internet or downloading software, consumers consider the playing of a CD to be a private and passive act and one that carries no risk of attack from the outside world. When security and privacy threats intruded upon this zone of safety, consumers reacted with unexpectedly intense indignation. The particularly strong reaction may also have stemmed from the lack of any perceptible fair trade-off between the benefits gained by consumers and the risks they faced. A user who downloads a free game or screensaver from the internet may suspect a risk of unwanted adware, but justifies that risk by the benefit of a free program. Here customers paid the expected price, and not only received less than they bargained for in terms

148. *Id.* at 28, 33.

149. For an overview of surveys and experiments revealing divergence in consumers' privacy attitudes from their behavior during transactions, see Alessandro Acquisti & Jens Grossklags, *Privacy Attitudes and Privacy Behaviors: Losses, Gains, and Hyperbolic Discounting*, in THE ECONOMICS OF INFORMATION SECURITY 165 (L. Jean Camp & Stephen Lewis eds., 2004). For specific examples of this phenomena, see Sarah Spiekermann, Jens Grossklags, & Bettina Berendt, *E-privacy in 2nd Generation E-commerce: Privacy Preferences Versus Actual Behavior*, in PROCEEDINGS OF THE 3RD ACM CONFERENCE ON ELECTRONIC COMMERCE 38-47 (2001) (discussing lab study finding inconsistencies between participants' self-reported privacy concerns and behavior in online shopping experiences).

of CD functionality, but were also saddled with undisclosed privacy and security risks.

XCP and MediaMax presented unique marketing challenges for Sony BMG. Since fully-informed customers were unlikely to pay full price for what they would view as an inferior product, Sony BMG faced a choice. It could either develop a product that included DRM but was nonetheless attractive to consumers—most likely by significantly reducing retail prices—or it could obfuscate the nature of the product it sold and prevent its customers from excising the unwanted DRM post-purchase. All evidence suggests that Sony BMG adopted the latter approach.

These same market conditions, however, existed for all major record labels, yet most of Sony BMG's competitors were content to implement less invasive technological protection measures, knowing full well that they would fail to prevent infringement.[150] The other major labels, unlike Sony, did not insist upon maximum effectiveness at the risk of harm to users.

The history of Sony, one of the two parent companies of Sony BMG, in its attempts to restrict access to and copying of its content may offer some insight into why Sony BMG, unlike its competitors, accepted these risks in return for an uncertain and at best marginal increase in the effectiveness of its DRM. The aggressive stance adopted by Sony in halting innovative consumer-driven uses of products like the Aibo robotic dog[151] and the Playstation[152] suggest a willingness to seek maximum protection of Sony intellectual property, even at the risk of consumer alienation.

---

150. *See* Jefferson Graham, *CD Woes May Have Had Roots in Merger*, USA TODAY, Nov. 18, 2005, at 1B. Some have suggested that shifts in management and massive staff cuts at Sony BMG may have contributed further to the breakdown that led to the release of XCP. *See id.*

151. The Aibo, which retailed for $1299, came preprogrammed with a limited set of functions. John G. Spooner, *Sony Aibo to Spread More Puppy Love*, CNET NEWS.COM, Oct. 10, 2002, http://news.com.com/2100-1040-961536.html. One enterprising Aibo owner and hobbyist decrypted the software code that defined the Aibo's abilities and distributed new software to Aibo owners that "taught" the dogs to dance and speak, among other things. David Labrador, *Teaching Robot Dogs New Tricks*, SCIENTIFIC AMERICAN.COM, Jan. 21, 2002, http://www.sciam.com/print_version.cfm?articleID=0005510C-EABD-1CD6-B4A8809EC588EEDF. Despite the fact that the software was of use only to Aibo owners and arguably increased the product's value, Sony demanded removal of the software, contending that decryption of the Aibo code violated the DMCA. *Id.*

152. When Connectix developed its Virtual Game Station, a software emulator that enabled owners of Sony PlayStation games to play titles on Apple computers, Sony filed a copyright infringement suit, alleging that Connectix, by reverse engineering Sony's game console, infringed the copyright in the PlayStation BIOS. Sony Computer Entm't

In light of this corporate heritage, the difficulty of convincing consumers of the value of DRM-protected CDs, and its underestimation of public reaction to degraded security and privacy, Sony BMG's decision to deploy XCP and MediaMax, its attempts to cloak its technology and its failures of disclosure emerge as explicable, if irresponsible, reactions to market conditions. But while its motivations are apparent, the long-term strategic benefit of this approach is difficult to discern, especially with the benefit of hindsight. The limitations and strengths of both the CD and the personal computer as platforms for the dissemination and playback of content, which we examine next, constrained and enabled Sony BMG's choices, further explaining, but not excusing, its actions.

IV. THE ROLE OF TECHNOLOGY

The technological landscape encouraged Sony BMG's decision to deploy its DRM through stealth measures. The personal computer, in theory, allows users broad choice over the operating system and applications that run upon it. The universal nature of the PC sits in stark contrast to the single-purpose devices historically used by individuals to enjoy music. This flexibility limits the control that Sony BMG and other copyright owners

---

Am., Inc. v. Connectix Corp., 203 F.3d 596, 598-99 (9th Cir. 2000). After the Ninth Circuit reversed the district court's finding of infringement, *id.* at 609-10, Sony acquired all rights to the Virtual Game Station from Connectix and ceased development rather than allow consumers to access its games on a competitor's platform. Phillip Michaels, *Emulation Sensation: Microsoft Buys Virtual PC from Connectix*, MACWORLD, May 2003, at 25, 25, *available at* 2003 WLNR 8626928. Sony also filed suit against Bleem, the manufacturer of a PC-based PlayStation emulator, claiming that by using screenshots of Sony games in its advertising, Bleem infringed Sony's copyrights. The Ninth Circuit vacated the district court's preliminary injunction, holding that Bleem's use was likely fair. Sony Computer Entm't Am., Inc. v. Bleem, LLC, 214 F.3d 1022, 1029 (9th Cir. 2000).

After the release of the PlayStation 2, Sony brought suit against Gamemasters, the manufacturer of the Game Enhancer, a device that enabled PlayStation owners to play games from other countries by bypassing region code restrictions encoded on game discs. Sony Computer Entm't Am., Inc. v. Gamemasters, 87 F. Supp. 2d 976 (N.D. Cal. 1999). Sony succeeded in obtaining a preliminary injunction on both contributory infringement and anti-trafficking theories, precluding U.S. customers from playing games legally purchased in Asia and Europe. *Id.* at 989.

In hopes of exerting further control over the video game aftermarket, Sony obtained a patent in connection with its latest video game console, the PlayStation 3, on a technology that would tie each copy of a game to a single console, effectively eliminating the resale and rental market for PlayStation 3 games. Dawn C. Chmielewski, *Furor Over Sony Patent: Technology That Could Prevent Resale of Games and Other Digital Goods Raises Speculation, Fears*, L.A. TIMES, July 10, 2006, at C1. That technology has yet to be implemented.

can exert over the applications that will be used to access and copy their CDs. As a result of the inability to control the platform for content delivery, Sony BMG was encouraged to consider preemptively limiting potential infringement through the use of invasive software countermeasures. Further complicating efforts to control content, the music industry's longtime distribution medium of choice, the CD, is an unencrypted format. These inescapable features of the playback device and distribution medium encouraged the adoption of invasive DRM techniques such as those employed by Sony BMG.

Technology not only animated Sony BMG's strategy, it also enabled it. Sony BMG likely banked on its ability to keep the existence and functionality of its DRM relatively secret from the general public. The rootkit itself was designed to maintain secrecy, but equally importantly, the standard configuration of many personal computers allows third parties to surreptitiously install code, including the DRM at issue here, without alerting the user or requiring affirmative steps to proceed with installation.

A. Technology as Encouragement

In conjunction, two features of the technological landscape encouraged, if not required, the use of intrusive technological protection measures such as those employed by Sony BMG. Given the combination of a general purpose, multifunctional networked playback device with an entrenched but unencrypted digital distribution medium, the music industry's adoption of software-based technological protection measures seems, in hindsight, unavoidable.

1. The PC as Playback Device

From the perspective of many copyright holders, the PC is perhaps the least-desirable device imaginable for the playback of unprotected CDs. Unlike the single-purpose devices that consumers have traditionally used to listen to music, the PC is a general-purpose device, a machine with nearly unbounded functionality, limited primarily by the software running on it. As a result, PC users are able to not only listen to the music contained on a CD, but to copy, transcode, edit, remix, and distribute it as well.

Contrast this range of user freedoms with those permitted by analog playback devices like the phonograph—particularly in the days before reel-to-reel and cassette recorders—and modern digital playback devices, like the DVD player. Phonograph users, even well into the twentieth century, were constrained in their ability to make copies of recordings by the

dictates of the state of the art—the equipment required to press phonograph records was simply not feasible for consumer use.

While the limitations of early analog media were primarily the result of engineering hurdles that would be overcome by subsequent innovations, limitations on modern digital playback devices are largely the result of intentional design decisions targeted at curtailing the relative ease of digital copying. The functionality of DVD players, for example, is tightly controlled by the DVD Copy Control Association (DVD CCA), the industry body that licenses the Content Scramble System (CSS) and holds the keys necessary to manufacture devices and software that legally play DVDs. Indeed both the DVD medium and its playback devices were designed from the ground up to permit increased control over consumer use of content. By insisting that CSS licensees conform to rigid specifications, content owners enjoy some increased assurance that devices that copy DVDs will not be appearing on store shelves any time soon. And when its licensees offer product features that test the bounds of this control, the DVD CCA has brought suit to maintain its grip over the medium.[153]

Unlike the DVD player, the personal computer was not developed with copy control and content protection in mind. Computer users are free to add or replace hardware, to substitute one operating system for another, and to install or uninstall software—or, if sufficiently skilled, to write their own. A system that permits this level of flexibility does not lend itself to the sort of control to which copyright holders aspire when designing playback devices. Any restriction imposed by software can be removed by software. As a result, skilled and determined users are capable of defeating any software-based content protection scheme deployed on a standard PC.

In recognition of this fact, content owners have sought to embed protection measures at deeper levels of the machine's architecture. The development of trusted computing platforms was in essence an attempt to reinvent the PC in a manner that wrested control from the hands of users and entrusted it to hardware manufacturers, software developers, and content owners.[154] While some touted this approach for its potential security

153. Kaleidescape, the producer of a high-end home entertainment server that allowed customers to store hundreds of DVDs on a networked device, prevailed in a lawsuit alleging that it violated the terms of its DVD CCA license. Transcript of Proceedings at 66, 67, 70, DVD Copy Control Ass'n, Inc. v. Kaleidescape, Inc., No. 1-04-CV031829 (Cal. Sup. Ct. Mar. 29, 2007), *available at* http://www.kaleidescape.com/files/legal/DVDCCA-vs-Kaleidescape-Statement-of-Decision.pdf.

154. *See* Ross Anderson, *Cryptography and Competition Policy—Issues with "Trusted Computing,"* at 3-5, http://www.cl.cam.ac.uk/~rja14/Papers/tcpa.pdf; *see also*

benefits, others suspected that DRM was the true driving force behind trusted computing.[155] Microsoft's Palladium, for example, was intended to take advantage of specially developed Intel hardware to integrate digital rights management into the CPU itself.[156] By embedding features like remote attestation,[157] sealed storage,[158] and memory curtaining[159] into the trusted computing environment, this approach held some promise for content owners who hoped to exercise greater control over copyrighted material on PCs. But despite widespread adoption of the Trusted Platform

---

Chad Woodford, Comment, *Trusted Computing or Big Brother? Putting the Rights Back in Digital Rights Management*, 75 U. COLO. L. REV. 253 (2004).

155. *See id.*

156. Electronic Privacy Information Center, Microsoft Palladium - Next Generation Secure Computing Base, http://www.epic.org/privacy/consumer/microsoft/palladium.html (last updated Nov. 11, 2002).

157. Remote attestation is a process by which software authenticates itself to a remote host. The user's local machine would share information about its hardware and software configuration in order for a remote machine to determine whether it will be trusted. Vivek Haldar et al., *Semantic Remote Attestation - A Virtual Machine Directed Approach to Trusted Computing*, *in* USENIX ASS'N, PROCEEDINGS OF THE THIRD USENIX VIRTUAL MACHINE RESEARCH & TECHNOLOGY SYMPOSIUM 29 (2004), *available at* http://www.usenix.org/events/vm04/tech/haldar/haldar.pdf. For example, users whose machines contained unauthorized software could be refused access by a remote website or service.

158. Sealed storage is a means by which the cryptographic keys necessary to access encrypted data are generated by authorized software rather than stored in the open on the user's machine. This approach is meant to ensure that content cannot be accessed by unauthorized software that could circumvent the limits imposed by authorized software. SETH SCHOEN, TRUSTED COMPUTING: PROMISE AND RISK (2003), http://www.eff.org/Infrastructure/trusted_computing/20031001_tc.pdf; Arnd Weber & Dirk A. Weber, *Legal Risk Assessment of Trusted Computing. A Review*, INDICARE MONITOR, Feb. 24, 2006, at 58, *available at* http://www.indicare.org/tiki-download_file.php?fileId=174.

159. Memory curtaining is a technique that prevents one application from accessing the memory used by another application, preventing, for example, unauthorized programs from capturing content being played by an authorized program that enforces restrictions on use of that content. SCHOEN, *supra* note 158; *see also* Mike Burmester & Judie Mulholland, *The Advent of Trusted Computing: Implications for Digital Forensics*, *in* ACM ASS'N, PROCEEDINGS OF THE 2006 SYMPOSIUM ON APPLIED COMPUTING 283 (2006), *available at* http://www.cs.fsu.edu/~burmeste/tc.pdf. There are stronger methods for isolating memory and resources. Andrew Whitaker, Marianne Shaw, and Steven D. Gribble, *Scale and Performance in the Denali Isolation Kernel*, ACM SIGOPS OPERATING SYS. REV, Winter 2002, at 195, *available at* http://portal.acm.org/citation.cfm?doid=844128.844147.

Module specifications,[160] trusted computing has yet to yield any radical transformation of the computing environment.

2. The Lack of an Encrypted Format

For the majority of its nearly 30-year history, the Compact Disc format, first developed in the late 1970s by Philips and Sony, has enabled consumers to freely access and copy CD content.[161] The CD, unlike later-developed digital formats like the DVD,[162] includes no content encryption.[163] Digital audio tracks on CDs can be read and copied by any compatible hardware, even in the absence of any cryptographic key. But by the late 1990s, after recordable CD media and hardware became commonplace and use of peer-to-peer networks became widespread, copyright holders sought to exercise greater control over the post-sale use of CDs. Given the massive user base of the CD and the investments of both content owners and consumer electronics manufacturers in the format, record labels faced a difficult task. They needed to devise methods to prevent unwanted PC-based copying while simultaneously maintaining usability on standard audio equipment. This required grafting protection measures onto a preexisting unencrypted format while retaining backwards compatibility.

Two general approaches to this problem emerged and can be broadly categorized as either passive or active. Passive protection measures rely on changes to the structure and data contained on the CD to prevent copying.[164] Active protection measures, like XCP and MediaMax, on the other hand, rely on the installation of software on the user's computer to interfere with the accessing and copying of audio files.[165]

---

160. For details on the Trusted Platform Module specifications, see Trusted Computing Group, Trusted Platform Module (TPM) Specifications, https://www.trustedcomputinggroup.org/specs/TPM (last visited July 30, 2007).

161. *See* J. Alex Halderman, *Evaluating New Copy-Prevention Techniques for Audio CDs*, *in* ACM ASS'N, PROCEEDINGS OF THE 2002 ACM WORKSHOP ON DIGITAL RIGHTS MANAGEMENT 101 (2002), *available at* http://www.cs.princeton.edu/~jhalderm/papers/drm2002.pdf.

162. The vast majority of commercially available DVDs utilize CSS, a method of encryption meant to ensure that only authorized devices and software can be used to access content. The DVD CCA's tight control over licensing of the keys necessary to access DVDs has successfully prevented the distribution of devices that enable users to copy DVDs. *But see DVD Copy Control Ass'n, Inc.*, *supra* note 153.

163. *See* Halderman, *supra* note 161.

164. For a study of the effectiveness of passive protection measures, see *id.*

165. Halderman & Felten, *supra* note 11, at 4.

Each song on a CD is stored as an individual track. Each track comprises a number of frames, each of which holds 1/75 second of audio.[166] In addition, parallel data streams, called subchannels, are multiplexed with each track's main data.[167] These subchannels mark the divisions between tracks, the track number, and the current track running time.[168] Aside from the track data, each CD contains a table of contents (TOC) which indicates the number of tracks and the starting position of each track.[169]

By introducing errors into CD data and the TOC, passive protection measures attempt to exploit subtle differences in the hardware and software of standard audio equipment and PCs.[170] For example, because the CD specification requires a two second gap before the beginning of the first track,[171] many PC CD drives specify time 00:02.00 as frame 0. By altering a TOC to indicate that the first track starts at time 00:01.74, passive protection measures can cause failure when a PC attempts to read the disc.[172] But since standard CD players use a different frame address scheme, the altered TOC typically does not interfere with playback.[173] Other passive measures rely on changes to the track data itself. Most CD players, for example, interpolate over errors caused by corrupt audio samples.[174] But since most PC CD-ROM drives cannot correct for such errors, by intentionally including corrupt samples, passive measures can interfere with the ability of PC drives to properly read protected discs without affecting playback on standard audio equipment.[175]

For a variety of reasons, passive protection measures proved to be at best an incomplete solution. First, some common audio components were unable to play back CDs with passive protection. Car stereos and DVD players with CD playback functionality often encountered difficulties with passively protected discs.[176] Second, not all PC drives were susceptible to

166. *Id.*
167. *Id.*
168. *Id.*
169. Halderman, *supra* note 161.
170. *Id.*
171. *Id. See also* INTERNATIONAL STANDARD NO. 60908, Audio Recording—Compact Disc Digital Audio System (Int'l Electrotechnical Comm'n 1999).
172. Halderman, *supra* note 161.
173. *Id.*
174. *Id.*
175. *Id.*
176. Will Knight, *Philips Says Copy-Protected CDs Have No Future*, NEW SCIENTIST, Jan. 11, 2002, http://www.newscientist.com/article.ns?id=dn1783; *Sony's 'Copy-Proof' CD Fails to Silence Hackers*, USA TODAY, May 20, 2002, http://www.usatoday.com/money/tech/2002-05-20-copyproof-cd.htm.

the rather crude methods relied upon by passive protection.[177] And as these methods became more prevalent, new drives were designed to eliminate the shortcomings of earlier hardware.[178] Even for computer users whose drives had difficulty reading passively protected discs, the careful application of tape or a felt tip pen could defeat passive DRM.[179] As a result, passive protection was largely abandoned in favor of active protection measures, which leave audio playback devices wholly undisturbed while providing greater and more flexible control over PCs.[180] However, unlike passive protection measures, active protection measures introduced an additional difficulty for content owners and developers of protection measures: since active measures operate by means of software running on users' machines, these measures needed to guarantee the installation of software most users would reject if given the choice. Luckily for copy protection proponents, the Windows computing environment made such installation without consent surprisingly easy.

B. Technology as Enablement

Technology not only motivated Sony BMG's choice to deploy invasive software-based DRM, but also provided the means to execute this strategy. Once installed, the rootkit itself helped to ensure that average consumers remained unaware of the software Sony BMG had installed on their machines. What enabled the stealth installation of the DRM software in the first place, however, was a standard feature of the dominant PC operating system: Sony BMG relied on the AutoRun feature of the Windows operating system to run and install code on users' machines without notice or consent.

AutoRun allows software code contained on removable media, like CDs, to run automatically when inserted into a computer. When a CD is inserted into a computer, Windows scans the disc for a file named "AutoRun.inf."[181] If that file is present, Windows faithfully executes its instructions.[182] The file could instruct the computer to launch a program, open a particular website, or take some other more harmful action. Despite the

177. *See* Halderman, *supra* note 161.

178. Halderman & Felten, *supra* note 11, at 8.

179. *See* Halderman, *supra* note 161.

180. Some later discs used a combination of active and passive protection measures. Edward W. Felten & J. Alex Halderman, *Digital Rights Management, Spyware, and Security*, IEEE SECURITY & PRIVACY, Jan.-Feb. 2006, at 18, *available at* http://www.computer.org/portal/cms_docs_security/security/2006/v4n1/18-23.pdf.

181. Halderman & Felten, *supra* note 11, at 5.

182. *Id.*

potentially destructive power ceded by AutoRun, Microsoft included no meaningful safeguards for computer users.

Using AutoRun, Sony BMG was able to install DRM software on computers without the knowledge or consent of users. Upon insertion of an XCP disc, AutoRun launched an installer program that presented users with the terms of the XCP EULA. If the user "accepted" the EULA terms, XCP installed software to play the CD and copy DRM-protected Windows Media files. These files, unlike MP3 files, cannot be copied to Apple's iPod or other portable media players. If a user instead rejected the EULA, the CD was ejected from the machine. Furthermore, if a user launched an audio program prior to accepting the EULA and installing XCP, the auto-launched installer gave the user thirty seconds to exit that program before the disc was ejected.[183] For many, if not most, users, this procedure meant that the only way to listen to a protected disc on a computer was to install XCP.

MediaMax employed even more aggressive tactics with the help of AutoRun. When inserted, MediaMax discs used AutoRun to install, without notice or consent, a device driver that altered the user's CD-ROM drive to prevent playback of MediaMax discs. Next, the installer presented the EULA. If accepted, the MediaMax software was installed. But if the user instead refused the terms of the EULA, the disc was ejected. Even if the user refused to accept the EULA, and the CD was ejected, SunnComm's MediaMax technology often remained installed on the user's computer—saddling users with all of the security and privacy vulnerabilities but providing no access to the music they purchased.[184]

In the face of predictable user reluctance to actively impede their own lawful uses of legally purchased CDs, Sony BMG and its DRM vendors leveraged the dominant operating system's lack of end user control over software installation decisions to clandestinely alter the personal computing environment of millions of users. In doing so, Sony BMG relied in part on methods used by spyware distributors to spread malicious code and seize remote control of users' computers. Arguably, the decision to use these stealth techniques was motivated by the same desires—limiting user knowledge, engagement, and choice—that motivate their use in the spyware and malware contexts.

Sony BMG's use of these techniques occurred against a backdrop of efforts by companies, including Microsoft, to bolster user control over

183. *Id.* at 6.
184. *Id.* at 7.

software installation through industry-wide efforts to create more meaningful and effective consent mechanisms[185] and product design to prevent the installation of spyware.[186] These efforts recognized that the categorization of products as malware or spyware depends as much on the consent experience and on satisfying user expectations as it does on a product's functionality. Since the rootkit incident, Microsoft has taken at least one step that increases end user control over software installation. In Windows Vista, its most recent operating system, Microsoft has altered the AutoRun mechanism. On first encounter with an AutoRun disc, the user has the opportunity to permit or deny the automatic execution of code and can set defaults for future AutoRun discs.[187] The lessons learned from Sony BMG's decision to use AutoRun, and its misuse in other "drive-by" download exploits no doubt influenced this redesign. It is more consistent with the principles of usable security discussed below, and will likely assist users in avoiding the installation of some insecure software.

V. EXISTING LAW AND SKEWED INCENTIVES

Sony BMG has paid dearly for its deployment of XCP and MediaMax through the investigations, litigation, and settlements that came in the wake of the rootkit incident.[188] The example made of Sony BMG will

185. The difficult of delineating "spyware" solely on the basis of software behavior has led legislators and industry to focus increasingly on the quality of the notice and consent procedures around a software program's installation in addition to its behavior. The Anti-Spyware Coalition's Best Practices Guide is an example of this revival of interest in constraining reasonable notice and consent mechanisms and procedures. *See* ANTI-SPYWARE COALITION, BEST PRACTICES: GUIDELINES TO CONSIDER IN THE EVALUATION OF POTENTIALLY UNWANTED TECHNOLOGIES (2007), *available at* http://www.antispywarecoalition.org/documents/documents/best_practices_final_working_report.pdf.

186. *Id.*; ANTI-SPYWARE COALITION, BEST PRACTICES: FACTORS FOR USE IN THE EVALUATION OF POTENTIALLY UNWANTED TECHNOLOGIES (2007), *available at* http://www.antispywarecoalition.org/documents/documents/best_practices_public_comment_draft.pdf.

187. MICROSOFT CORPORATION, WINDOWS VISTA SECURITY GUIDE ch. 3 (2006), http://www.microsoft.com/technet/windowsvista/security/protect_sensitive_data.mspx; CD AutoRun Basics: Windows Vista AutoPlay and AutoRun, http://www.phdcc.com/shellrun/AutoRun.htm#vista (last modified Dec. 19, 2006).

188. *See, e.g.*, Settlement Agreement, *supra* note 69; Robert McMillan, *Second Sony Rootkit Settlement Ups Payout to $5.75M*, COMPUTER WORLD, Dec. 21, 2006, http://www.computerworld.com/action/article.do?command=viewArticleBasic&articleId=9006620; Agreement Containing Consent Order, *In re* Sony BMG Music Entm't, FTC File No. 062 3019 (Jan. 30, 2007), *available at* http://www.ftc.gov/os/caselist/0623019/070130agreement0623019.pdf.

likely shape future DRM deployments by injecting security considerations into their development and by influencing notice and consent practices.[189] These developments, as we discuss in Part VI, provide a solid foundation for broader interdisciplinary efforts to improve privacy and security in the online environment. But rather than analyze the sufficiency of the price paid by Sony BMG for its misdeeds, we seek to understand why existing law failed to prevent the deployment of DRM with known security and privacy risks. In hindsight, it is apparent that Sony BMG's decision to deploy its DRM was woefully misguided, and that the statements about its data collection were inaccurate and incomplete. Assuming Sony BMG had competent legal counsel, the question is why the law failed to clearly alert Sony BMG of the illegality of this strategy. Equally important is an understanding of the failure of the law to empower users with the information and control to avoid these security and privacy risks.

A complicated picture emerges. We contend in Section V.A that Sony BMG's likely reliance on the hidden nature of the DRM's functionality was buttressed in part by the Digital Millennium Copyright Act's anti-circumvention rules, which discourage experts from studying the security risks posed by technological protection measures. By exposing security researchers to liability for their research, the DMCA discourages the front-line of security defense in the online environment. The anti-trafficking rules similarly interfere with the distribution of information or tools that could assist users in disabling technological protection measures, like the Sony BMG DRM, in order to avoid risks to their privacy and security. Second, existing contract law has failed to set meaningful limits on the substance and formalities of click-wrap contracting. The unwillingness of courts to set substantive limits on EULAs and to critically consider the consent experience created an environment in which unreasonable material terms can be inserted into EULAs with impunity. And without a meaningful consent experience, users cannot even hope to have notice of the terms foisted upon them by these mass-market form contracts. Third and finally, the focus of U.S. privacy initiatives on a narrowly defined class of "personally identifiable information" created uncertainty about privacy rules for businesses using unique identifiers, such as IP addresses, to identify or monitor users. By discouraging security research on technological protection measures, failing to take a hard look at the terms and

189. Pamela Samuelson & Jason Schultz, *Regulating Digital Rights Management Technologies: Should Copyright Owners Have to Give Notice About DRM Restrictions?*, J. TELECOMM. & HIGH TECH. L. (forthcoming 2007) (manuscript at 17, available at http://www.ischool.berkeley.edu/~pam/papers/notice%20of%20DRM-701.pdf).

formalities of "click-wrap" agreements, and neglecting to provide guidance on privacy issues beyond those arising with "personal identifying information," courts and regulators failed to strike the appropriate balance between commercial convenience, on the one hand, and consumer protection and empowerment, on the other.

A. The DMCA's Veil of Secrecy

At present, federal law does not explicitly endorse invasive attacks by copyright holders against the computers of suspected infringers. Proposals like H.R. 5211, introduced by Representative Howard Berman in 2002, would have enabled such self-help hacking in the name of enforcing intellectual property rights.[190] Congress rightly rejected this approach.[191] But even in the absence of any official congressional imprimatur on invasive self-help, Congress has created a set of disincentives through the DMCA that, if not appropriately checked, could yield the same result—namely, unrestrained and overzealous copyright enforcement mechanisms that endanger the security of personal computers and the network generally.

This Section considers the implications of the DMCA on the security researchers who serve as the primary source of information regarding abusive protection measures for the public, law enforcement, and regulators. By imposing potential liability for discovery, disclosure, and deactivation of harmful protection measures, the DMCA was perhaps the primary component of the legal framework that failed to prevent the rootkit incident.

In the weeks and months prior to the public disclosure of the XCP rootkit, two prominent computer security and DRM researchers, Professor Ed Felten and J. Alex Halderman, were forced to divide their energy between researching and publicizing the dangerous implications of Sony BMG's protection measures, on the one hand, and engaging in protracted discussions of potential DMCA liability with both their outside legal team and the general counsel of their academic institution, on the other.[192] The

---

190. H.R. 5211, 107th Cong. (2d Sess. 2002), *available at* http://thomas.loc.gov/cgi-bin/query/z?c107:H.R.5211:.

191. Legislative History of H.R. 5211, 107th Cong. (2002), http://thomas.loc.gov/cgi-bin/bdquery/z?d107:HR05211:@@@X.

192. Halderman and Felten were clients of the Samuelson Law, Technology & Public Policy Clinic directed by Mulligan. Perzanowski was the student most intimately and continuously involved in advising Halderman and Felten. Clinic Fellow Jack Lerner and clinic student interns Sara Adibisedeh, Azra Medjedovic, and Brian W. Carver all participated in the representation at various times. Joseph Lorenzo Hall, a Ph.D student at Berkeley's Information School and a long-standing participant in the Samuelson Clinic's

caution displayed by Halderman and Felten is hardly surprising given their personal histories with the DMCA. Both have been threatened with legal action in the past and are therefore acutely aware of the exacting toll of litigation threats, regardless of the merits of the claims.[193] But the necessary delay caused by legal uncertainty left millions at risk for weeks longer than necessary.

In broad terms, the DMCA undergirds the technological protection measures adopted by copyright holders with the force of law. The statute prohibits circumvention of any measure that effectively protects access to a copyrighted work.[194] In addition, the DMCA imposes liability on those who traffic in tools, devices, components, or services primarily designed, marketed, or commercially viable only for the purpose of circumventing protection measures that control access to or copying of copyrighted works.[195] Both the anti-circumvention and anti-trafficking provisions of the DMCA contribute to the ominous shadow that hangs over researchers examining the security of any product protected by a technological protection measure,[196] a pall most strongly felt by those examining the protection

---

research, provided technical advice and support to law students working on this project. As Felten and Halderman wrote, "Sadly, research of this type does seem to require support from a team of lawyers." As much as the lawyers enjoyed the privilege of working with and representing interesting people doing important work, they share their former clients' dismay at this particular state of affairs.

193. In 2000, Felten and a team of researchers, after accepting a challenge from the Secure Digital Music Initiative (SDMI), succeeded in breaking SDMI's digital audio watermark. After facing legal threats under the DMCA, Professor Felten filed for declaratory judgment seeking a determination that his research did not violate the DMCA. Only after the RIAA disavowed any intent to file suit was that action dismissed. *See Tinkerers' Champion*, THE ECONOMIST, June 22, 2002; First Amended Complaint, Felten v. Recording Indus. of Am., Inc., No. CV-01-2660 (D.N.J. June 26, 2001), *available at* http://www.eff.org/IP/DMCA/Felten_v_RIAA/20010626_eff_felten_amended_complaint.html.

In 2003, Halderman published an academic paper discussing his research on SunnComm's MediaMax protection measure. *See supra* note 4. Shortly thereafter, SunnComm threatened Halderman with legal action for his academic publication. Kevin Maney, *Debate Heats Up as Student Spots Hole in CD Protection*, USA TODAY, Oct. 27, 2003, at 1A. After scathing criticism of its attempt to silence legitimate research, SunnComm publicly retracted this threat. *See* Lisa Napoli, *Compressed Data; Shift Key Opens Door to CD and Criticism*, N.Y. TIMES, Oct. 13, 2003, at C3.

194. 17 U.S.C. § 1201(a)(1)(A) (2000).

195. 17 U.S.C. § 1201(a)(2), (b)(1) (2000).

196. *See generally* Chamberlain Group, Inc. v. Skylink Techs., Inc., 381 F.3d 1178 (Fed. Cir. 2004); Lexmark Int'l, Inc. v. Static Control Components, Inc., 387 F.3d 522 (6th Cir. 2004).

measures applied to creative works—music, movies, novels—that the DMCA was intended to protect.[197]

In their efforts to determine the security threats posed by DRM systems like XCP and MediaMax, researchers are likely to disable or remove some portion or the entirety of the protection measure, and thus potentially run afoul of the DMCA's prohibition against circumvention.[198] Assuming researchers—and their institutions—are willing to accept these risks, they could face further threats of litigation for publishing the results of their research. To the extent that publication of sufficiently detailed findings enabled others to circumvent the protection measure, it could lead to claims of trafficking. Although such claims are unlikely to succeed,[199] the

197. As discussed *supra*, the Digital Millennium Copyright Act (DMCA) has been used to threaten academic research. But the chilling effect of the DMCA has extended far beyond security research. It has impeded tinkering with online games and gadgets and interfered with online speech. *See supra* notes 151 and 152; ELECTRONIC FRONTIER FOUNDATION, UNINTENDED CONSEQUENCES: SEVEN YEARS UNDER THE DMCA (2006), http://www.eff.org/IP/DMCA/DMCA_unintended_v4.pdf.

Nor is the DMCA the only legal barrier to improving computer security. Bucking the call for growing scrutiny and improvement of electronic voting technology, dominant election system vendors have used the threat of legal action based on intellectual property violations to interfere with competition, impede the review of electronic systems by regulators, and chill public discourse about the lax security of their machines. For an overview of the issues faced by election officials see AARON BURSTEIN ET AL., SAMUELSON LAW, TECHNOLOGY & PUBLIC POLICY CLINIC, LEGAL ISSUES FACING ELECTION OFFICIALS IN AN ELECTRONIC-VOTING WORLD (2007), http://www.law.berkeley.edu/clinics/samuelson/projects_papers/Legal_Issues_Elections_Officials_FINAL.pdf.

198. The great irony, of course, is that although during the exploration of the security risks posed by the DRM researchers are likely to disable or remove some portion or the entirety of the protection measure, and thus potentially run afoul of the DMCA, engaging in such research does not constitute copyright infringement. Indeed, security researchers are concerned with the manner in which protection measures function and the security threats they may pose; they have no interest in the copyrighted content those measures are meant to protect.

199. Statements made by the Department of Justice in *Felten v. RIAA* are instructive. In that case, the DOJ argued against an interpretation of "tools" that would include "normal scientific research" and publishing. Defendant John Ashcroft's Memorandum in Support of Motion to Dismiss, at 17, Felten v. Recording Indus. Ass'n of Am., No. 01-CV-2669 (D.N.J. Sept. 25, 2001) ("[t]he Plaintiffs are scientists attempting to study access control technologies. The DMCA simply does not apply to such conduct."). The DOJ did reserve the possibility that "making available a publication that describes in detail how to go about circumventing a particular technology, if written or marketed for the express purpose of actually circumventing that technology," could be prosecuted under the statute. *Id.* at 17 n.5. Some cases involving defendants who publicly distribute and advertise what effectively amount to step-by-step instruction guides on how to commit crimes have resulted in successful prosecutions in other areas. *See, e.g.*, Rice v. The Pala-

threat of litigation and the associated expense is sufficient to alter research agendas. Finally, assuming researchers discovered a security flaw that posed a significant threat to the public, as in the case of Sony BMG's DRM, and sought to provide a tool to enable the average computer user to quickly and safely avoid the harms posed by the protection measure, they almost certainly would raise the ire of the content industry to a fever pitch and draw a trafficking claim under the DMCA. Together the anti-circumvention and anti-trafficking provisions chill computer security research and create enormous disincentives to provide the information and tools necessary to enable computer users to avoid security and privacy risks once dangerous technologies have been deployed.

A detailed analysis of potential liability under the DMCA and the ways in which it complicates research, publication, and the dissemination of tools related to DRM is beyond the scope of this Article.[200] Nonetheless, there are good reasons to doubt that liability should attach in these circumstances. First, the more enlightened courts to analyze the DMCA recognize that liability requires some nexus between the act of circumvention and an act of copyright infringement.[201] Where circumvention and

---

din Enters., 128 F.3d 233, 266-67 (9th Cir. 1997); United States v. Barnett, 667 F.2d 835, 842 (9th Cir. 1982). However, sharing general information about how to commit criminal acts that is unlikely to incite others to imminently take lawless action typically fails to justify restricting its expression. McCoy v. Stewart, 282 F.3d 626, 632 (9th Cir. 2002). Given that security research is not marketed for the purpose of circumvention, it is unlikely to be found to incite others to imminently commit unlawful acts.

200. As counsel to Halderman and Felten, the authors have conducted an exhaustive analysis of this issue.

201. Chamberlain Group, Inc. v. Skylink Techs., Inc., 381 F.3d 1178 (Fed. Cir. 2004), succinctly sets forth the applicable law on this point:

> A plaintiff alleging a violation of § 1201(a)(2) must prove: (1) ownership of a valid copyright on a work, (2) effectively controlled by a technological measure, which has been circumvented, (3) that third parties can now access (4) without authorization, in a manner that (5) infringes or facilitates infringing a right protected by the Copyright Act, because of a product that (6) the defendant either: (i) designed or produced primarily for circumvention; (ii) made available despite only limited commercial significance other than circumvention; or (iii) marketed for use in circumvention of the controlling technological measure.

Chamberlain Group, Inc., 381 F.3d at 1203; *accord* Storage Tech. Corp. v. Custom Hardware Eng'g & Consulting, Inc., 421 F.3d 1307 (Fed. Cir. 2005) (in order to prevail in a DMCA claim, the plaintiff must also be able to succeed on the merits in an underlying copyright infringement suit).

publication take place in the context of academic research, courts should be reluctant to find the requisite nexus.

Second, at least with respect to Sony BMG's DRM, it is far from clear that the technological protection measures at issue would have been found to "effectively control access" to the CDs.[202] Absent such a finding, research and subsequent publication, or even distribution of a tool, would not be actionable under the DMCA's anti-circumvention and anti-trafficking provisions.[203] In *Lexmark Int'l, Inc. v. Static Control Components, Inc.*, the Sixth Circuit explained that section 1201(a)(2) does not extend to a technological measure that restricts one form of access but leaves another route wide open.[204] XCP and MediaMax both left audio content unprotected and accessible by other obvious means.[205] Purchasers could access the tracks without restriction on their CD players, any Apple computer, or any Windows machine on which AutoRun was disabled.[206] Under these circumstances, the availability of DMCA protection is an open question.

---

202. Per the statute, "controls access to a work" means that if the measure, in the ordinary course of its operation, requires the application of information, or a process or a treatment, with the authority of the copyright owner, to gain access to the work. 17 U.S.C. § 1201(a)(3)(B) (2000).

203. 17 U.S.C. § 1201 (a), (b) (2000).

204. Lexmark Int'l, Inc. v. Static Control Components, Inc., 387 F.3d 522, 547 (6th Cir. 2004).

205. Some files, such as bonus video content or compressed audio files, are not accessible through these other means. But since removal of the protection measure does not grant access to these files, the fact that they remain protected cannot support a claim of circumvention.

206. DRM vendors and copyright holders would likely have argued that their controls are effective "in the ordinary course of its operation," i.e., in the environment in which they were intended to be used. This argument assumes that the DRM vendors have some authority to control the underlying configuration of a user's machine. Given that access to the audio files is not protected on some standard-configured Windows computers and on Macs, this argument would implicitly suggest that users with "normally configured" machines are engaged in illegal circumvention. To succeed on this argument, Sony BMG would have to convince the court to adopt the position that the licensor has the right to control the general computing environment in which the consumer makes personal use of the CD audio files. It is difficult to imagine this argument proving persuasive, given its rather radical and broad implications, and given that its adoption would run counter to the "no technology mandates" provision in the DMCA, which states: "Nothing in this section shall require that the design of, or design and selection of parts and components for, a consumer electronics, telecommunications, or computing product provide for a response to any particular technological measure . . . ." 17 U.S.C. § 1201(c)(3) (2000).

An additional wrinkle in the analysis of potential liability facing researchers arises from the security testing exemption in section 1201(j), which applies to both the anti-circumvention provision and the anti-trafficking provision of 1201(a). It is the only statutory exemption that could potentially shield security researchers who disable protection measures like XCP and MediaMax and traffic in tools that enable others to avoid security risks. However, the scope of this exemption is, at best, uncertain,[207] and its applicability to the rootkit incident and similar potential circumstances is unsettled. First, section 1201(j)(1) limits the definition of "security testing" to "accessing a computer, computer system, or computer network, solely for the purpose of good faith testing."[208] This definition may not apply to circumvention of technological measures that protect third party content stored on removable media, such as sound recordings on CDs, that are distinct from the computer, system, or network. The scant legislative history offers some support for this reading. Section 1201(j) was adopted to accommodate concerns raised by developers of firewalls who wanted to ensure that they, their customers, and their competitors could test the effectiveness of their products.[209] In addition, since the sole purpose of security research is not to "promote the security of the owner or operator," but rather to protect the security of the public broadly—a purpose that may require widespread publication of information regarding removing the protection measure at issue—this sort of research could run

207. Section 1201(j) has been given short shrift in judicial opinions addressing the DMCA. Aside from a passing and dismissive reference in *Universal City Studios v. Reimerdes*, 111 F. Supp. 2d 294, 321 (S.D.N.Y. 2000), the exemption has been ignored by both courts and litigants. What attention the *Reimerdes* court did pay to 1201(j) was marred by a misreading of the statute. The court held that because "defendants sought, and plaintiffs granted, no authorization for defendants' activities" § 1201(j) did not apply. *Id.* The leading academic interpreting the statute also finds that the statute requires authorization. *See* Pamela Samuelson & Suzanne Scotchmer, *The Law and Economics of Reverse Engineering*, 111 YALE L.J. 1575, 1648 n.339 (2002) ("The computer security exception requires that the researcher actually get, and not just ask for, permission to defeat the technical protection measure."). However, the statute requires authorization not from the copyright holder, but from the owner or operator of the computer. This *Reimerdes* court's reading is therefore almost certainly a misapplication of the statute.

208. 17 U.S.C. § 1201(j) (2000).

209. The Conference Report on the DMCA offers further support for this narrow reading of the definition of security testing under 17 U.S.C. § 1201(j). That report explained, "It is not unlawful to test the effectiveness of a security measure before it is implemented to protect the work covered under title 17. Nor is it unlawful for a person who has implemented a security measure to test its effectiveness." H.R. REP. NO. 105-796, at 67 (1998) (Conf. Rep.).

afoul of the statute.[210] As discussed *infra*, the scope of the security research exemption was sufficiently unclear to justify the Copyright Office's decision to grant a temporary exemption to enable research on security-flawed CD-based protection measures.

Even assuming a competent legal team and success on the merits, defending against a DMCA suit consumes enormous resources. The threat of litigation understandably chills security research related to DRM. Suppressing research of this sort disables an important check on the safety and soundness of products in the consumer marketplace. Just as Consumers Union and other independent analysis and benchmarking entities act as independent checks on quality and safety for consumer products, computer security researchers play an important role in evaluating the security, privacy, usability, and other consumer-relevant effects of software. Preventing computer security researchers from evaluating products that contain technological protection measures removes an important player in the market ecosystem with respect to consumer protection.

Without the efforts of security researchers who discovered and publicized the risks created by Sony BMG's DRM,[211] consumers and policymakers would be nearly universally uninformed about security threats and other unknown consequences of DRM—a fact likely well understood by copyright holders who choose to deploy stealth protection measures with undisclosed functionalities. The vast majority of computer users lack the expertise to discover these threats independently. There is no government agency that is explicitly authorized to examine DRM or other technological protection measures to assess their policy implications or ramifications—security or other—on behalf of consumers. As a result, consumers must either rely on the research conducted by security experts[212] or blindly trust software developers and content owners to exercise restraint in designing protection measures that respect consumers' privacy and security interests.[213]

---

210. 17 U.S.C. § 1201(j)(3) (2000).

211. *See supra* Section I.A.

212. The DMCA harms consumers not only by denying them the expertise of researchers, but also by imposing liability for self-help. Once some information regarding the existence and functionality of a protection measure becomes available, many enterprising users could remove it on their own. However, the DMCA creates threats against users as well as researchers.

213. Posting of Ed Felten & J. Alex Halderman to Freedom to Tinker, http://www.freedom-to-tinker.com/?p=927 (Nov. 15, 2005, 07:07 EST). The rootkit incident and the historic use of monitoring in online content distribution systems suggests that such reliance would be misplaced. Deirdre K. Mulligan et al., *How DRM-based Content Delivery*

B. The Insufficiency of Consent

Aside from the force of law conferred by the DMCA, Sony BMG's DRM scheme benefited from some degree of legal protection offered by its software licenses. These licenses arguably enabled Sony BMG to maintain that users of XCP and MediaMax assented to the installation and functionality of Sony BMG's DRM. But the vast majority of Sony BMG customers lacked any meaningful understanding of the functionality of these protection measures, in part as a result of Sony BMG's misleading license terms and in part because of deficiencies in the consent experience associated with click-wrap licenses generally. Despite these barriers to meaningful consent, under contemporary contract doctrine, most of the terms of the XCP and MediaMax EULAs would be enforced against users, further emboldening Sony BMG.

XCP and MediaMax, like almost all consumer software, were distributed under the terms of EULAs. Typically EULAs disclose, among other things, the data collection, advertising, and other program functionalities of software, and require a "click" or other affirmative act to acknowledge the user's consent to the terms. In the case of the Sony BMG DRM protected CDs, the EULAs contained false statements claiming that no personal information would be collected about the user or their computer.[214] Indeed, the EULA governing DRM-protected Sony BMG CDs explicitly disavowed any collection or dissemination of data related to customers or their computers. The XCP EULA stated in part "the SOFTWARE will not be used at any time to collect any personal information from you, whether

---

Systems Disrupt Expectations of "Personal Use", *in* ASS'N FOR COMPUTING MACHINERY, PROCEEDINGS OF THE 3RD ACM WORKSHOP ON DIGITAL RIGHTS MANAGEMENT 77 (2003).

214. The EULA stated, "[T]he SOFTWARE will not be used at any time to collect any *personal information* from you, whether stored on YOUR COMPUTER or otherwise." Sony BMG MediaMax EULA (emphasis added) (on file with authors). The use of the term "personal information", rather than "personally identifiable information", created exposure here for Sony BMG, as discussed *infra* in Section V.C. Information at the SunnComm Sony BMG customer care website further misleads consumers, stating, "*No information* is ever collected about you or your computer without you [sic] consenting" and also states: "Is any personal information collected from my computer during the digital key delivery process? No, during the digital key delivery process, no information is ever collected about you or your computer." Posting of J. Alex Halderman to Freedom to Tinker, http://www.freedom-to-tinker.com/?p=925 (Nov. 12, 2005, 12:30 EST) (emphasis added). The lack of *any* modifiers with respect to "information" is startling. This statement would prohibit any connection to a remote server. The lack of consistency in terminology across the documents and the failure to use existing legally accepted definitions to describe the data they were claiming not to collect proved exceedingly problematic.

stored on YOUR COMPUTER or otherwise."[215] The MediaMax license agreement contained similar language.[216] In fact, both the XCP and MediaMax DRM collected and transmitted to Sony BMG the user's IP address, the time the CD was played, and a code corresponding to the particular CD title being played. Additionally, the EULA contained a host of overreaching terms.[217] The most significant was a provision permitting Sony BMG to install and use backdoors in the DRM and media player to enforce its rights at any time and without notice to the user.[218] Like the security threats introduced by XCP and MediaMax, the overreaching, false, and confusing statements found in the EULA were of the sort typically associated with spyware.

Since components of Sony BMG's DRM installed—sometimes permanently—before customers were confronted with the EULA terms, the CD packaging provided the only available means of pre-installation notice. But the information conveyed by the packaging left much to be desired. It too failed to provide adequate information about the installation and functionality of the software. XCP-protected discs contained the IFPI "Content Protected" logo on the front of the CD jewel case spine[219] and a small "content protection grid," illustrated below in Figure 1, on their back covers.[220] The majority of MediaMax discs included similar grids.[221] Others featured ambiguous disclosures in miniscule type, buried within system requirements.[222] Some neglected to inform customers that the CD

215. Sony BMG XCP EULA (Jan. 7, 2005) (on file with authors).

216. "At no time will any information provided by you in connection with the installation of the software system be collected about you or your computer." Sony BMG MediaMax EULA, *supra* note 214.

217. *See supra* note 27.

218. "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." Sony BMG XCP EULA, *supra* note 215.

219. Electronic Frontier Foundation, *supra* note 57.

220. CD's Containing XCP Content Protection Technology, Sony BMG, http://cp.sonybmg.com/xcp/english/titles.html.

221. Electronic Frontier Foundation, *supra* note 57.

222. For a number of examples, see Gallery of Variations on SunnComm MediaMax CD Labeling, http://www.eff.org/IP/DRM/Sony-BMG/mediamaxpics.php (last visited Sept. 6, 2007).

would automatically install software on their systems,[223] while others failed to disclose any of the restrictions on copying or accessing content imposed by the MediaMax software.[224] These half-hearted disclosures failed to provide Sony BMG customers with fair warning of the security and privacy threats or the scope of the limitations on use imposed by its DRM.

Figure 1

Users who took the time to sift through the nearly 3000-word XCP EULA[225] gleaned some additional detail beyond the cursory notice provided on the CD packaging. But the EULA failed to fully disclose the security and privacy risks imposed by Sony BMG's protection measures. Once customers purchased CDs and attempted to listen to them using their computers, the EULA—assuming they read it[226]—informed them:

> 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

---

223. *See, e.g.*, http://www.eff.org/IP/DRM/Sony-BMG/img/cubanlink_close.jpg ("THIS CD IS ENHANCED WITH MEDIAMAX SOFTWARE AND PROTECTED AGAINST UNAUTHORIZED DUPLICATION.")

224. Some stated:

> This CD is enhanced with Media Max software . . . . Software will automatically install . . . . Usage of this CD on your computer requires acceptance of the End User License Agreement and installation of specific software contained on this CD . . . . Certain computers may not be able to access the enhanced portion of this disc. None of the manufacturer, developer, or distributor [sic] makes any representation or warranty, or assumes any responsibility, with respect to the enhanced portion of this disc.

See http://www.eff.org/IP/DRM/Sony-BMG/img/contraband_close2.jpg

225. Sony BMG XCP EULA, *supra* note 215.

226. Users frequently ignore or fail to read EULAs. Nathaniel Good et al., *User Choices and Regret: Understanding Users' Decision Process About Consensually Acquired Spyware*, 2 I/S: J.L. & POL'Y FOR THE INFO. SOC'Y. 283 (2006).

> an end user license agreement . . . . 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.[227]

So while the EULA informed users that a small program would be installed on their machines, it provided no information about the specific restrictions that program placed on use of the CD or the manner in which it operated. Even customers who proactively sought information about the XCP software had no way, short of installing the software and running sophisticated diagnostic tests,[228] to discover the security vulnerabilities it introduced or that its explicit assurances regarding the collection of personal information were false. The same held true for the MediaMax EULA.[229] All but the most sophisticated users were left to blindly trust Sony BMG's incomplete and misleading disclosures. By doing so, they unwittingly opened their PCs to crippling attacks and their personal information to collection and transmission, both in exchange for restricted access to the music they believed they had purchased.

Because the EULA did disclose, albeit poorly, provisions that provided for Sony BMG's backdoor access and remote control over the user's computer—the provisions posing the greatest threats to security—courts would likely enforce those terms.[230] While EULA language is typically far from clear, even for those familiar with legal documents, courts are reluctant to excuse violations on the basis of unclear language. Nor do courts excuse consumers from license obligations on the basis of their failure to read EULA terms. As a matter of contract formation, courts typically find

---

227. Sony BMG XCP EULA, *supra* note 215.

228. Exceedingly few users possess the software and know-how necessary to conduct the sort of investigation engaged in by Mark Russinovich or Felten and Halderman. *See* Mark's Blog, *supra* note 6; Halderman & Felten, *supra* note 11.

229. "In order to properly utilize this CD on your computer, it is necessary to install a small software program on your computer hard drive." Sony BMG MediaMax EULA, *supra* note 214.

230. *See* Jane K. Winn, *Contracting Spyware by Contract*, 20 BERKELEY TECH. L.J. 1345 (2005). The doctrine of unconscionability, while unlikely to succeed, would provide the strongest basis for voiding this particular term. The form contracting of the EULA, the unexpected behavior of the software, and the general surprise of consumers that any software at all was being downloaded on to their computer, along with the potential harm the consumer is exposed to would lend support to a finding of unconscionability.

that installing or using the software is sufficient to establish acceptance of EULA terms even when users are not required to click "I Agree."[231] Whether consumers actually read the EULAs or whether they were designed to encourage reading or comprehension is generally not of interest to courts. When a document is reasonably understood to create legal obligations, courts impose a duty to read.[232] This obligation to read extends not just to EULAs, but to documents hyperlinked from EULAs as well.[233] If users read and understood the terms of software EULAs, many would be surprised by the number of legal obligations they create. As with the bizarre terms in the Sony BMG license that prohibited use of the CDs on office computers and terminated the licensee's rights in the CD if it was stolen or if the user filed for bankruptcy, the restrictions and obligations created in EULAs are often incongruous with consumer expectations about the contents of these documents.[234]

Unless squarely at odds with public policy or deemed unconscionable, EULA terms are generally enforced. Unconscionability requires both procedural defects in the contract formation process and substantive terms

---

231. *See* Tarra Zynda, Note, Ticketmaster Corp. v. Tickets.com, Inc.*: Preserving Minimum Requirements of Contract on the Internet*, 19 BERKELEY TECH. L.J. 495, 504-05 (2004).

232. Heller Fin., Inc. v. Midwhey Powder Co., 883 F.2d 1286, 1292 (7th Cir. 1989).

233. Hubbert v. Dell Corp., 835 N.E.2d 113 (Ill. App. Ct. 2005). *Hubbert* was followed twice in Nadler v. Merlin Int'l, Inc., 2007 U.S. Dist. LEXIS 19651 (S.D. Ill. Mar. 20, 2007) and Provencher v. Dell, Inc., 409 F. Supp. 2d 1196 (C.D. Cal. 2006).

234. Nathan Good et al., *Noticing Notice: A Large-Scale Experiment on the Timing of Software License Agreements*, *in* 1 ASS'N FOR COMPUTING MACHINERY SPECIAL INTEREST GROUP ON COMPUTER-HUMAN INTERACTION, CONFERENCE ON HUMAN FACTORS IN COMPUTING SYSTEMS 607 (Bo Begole & Stephen Payne eds., 2007), *available at* http://www.ischool.berkeley.edu/~jensg/research/paper/Grossklags07-CHI-noticing_notice.pdf; Deirdre Mulligan et al., *Stopping Spyware at the Gate: A User Study of Privacy, Notice and Spyware*, *in* 93 ACM INTERNATIONAL CONFERENCE PROCEEDING SERIES: PROCEEDINGS OF THE 2005 SYMPOSIUM ON USABLE PRIVACY AND SECURITY 43 (2005). The overreaching and unexpected content of Sony BMG's EULA does not set it apart as an outlier. For example, after just a few clicks, a user installing a well-known and popular file-sharing program agrees to provisions that prohibit reverse engineering, disabling advertisements, and removing third party software; force them into mandatory arbitration; permit the sharing of the user's contact information and browsing history; and bind all subsequent users of the software to the EULA.

The iTunes EULA includes: "You also agree that you will not use these products for the development, design, manufacture, or production of missiles, or nuclear, chemical or biological weapons." Apple QuickTime 7.0.4 (free version for Windows) and iTunes EULA (on file with authors).

that unfairly oppress one party to the contract.[235] In the context of the Sony BMG EULA, many courts would not object to the formation process itself, given Sony BMG's use of current industry standard mechanisms like the scroll box and click through assent.[236] Nonetheless, research and experience show this process does not engage users in any meaningful way in the contracting process.[237] And, while the installation of software that can be remotely updated and can enforce Sony BMG's rights with respect to content sounds substantively problematic, it is consistent with the operation of other online content delivery systems for movies and music.[238] So embedding a term requiring users to consent to the installation of a backdoor allowing remote updates and ongoing access to the user's computer in a dense and lengthy EULA is not quite the aberration it seems to be, although we contend that it should be. This is, in fact, the direction in which content protection schemes in the PC environment are moving.[239] Although the security and privacy flaws created by the DRM could provide a basis for a substantive challenge to the EULA, unconscionability requires both substantive and procedural defects.

---

235. *See, e.g.*, Williams v. Walker-Thomas Furniture Co., 350 F.2d 445 (D.C. Cir. 1965).

236. *But see* Ting v. AT&T, 319 F.3d 1126, 1148 (9th Cir. 2002) ("[A] contract of adhesion, i.e., a standardized contract, drafted by the party of superior bargaining strength, that relegates to the subscribing party only the opportunity to adhere to the contract or reject it" is necessarily procedurally unconscionable).

237. Good et al., *supra* note 234.

238. *See* Mulligan et al., *supra* note 213 (discussing monitoring of user activities identified in EULAs and by monitoring program activities).

239. The general movement toward platforms and software that allow for remote attestation about software behavior is found in industry efforts around the creation of a trusted computing platform. This technology is designed to allow one party to verify the "state" and operations of another's machine. In the context of asset management, where a business wants to assure that all the machines remotely connecting to its network are configured in a manner that will protect business interests (personal information, intellectual property, etc.) remote attestation is a promising development. In the context of content owners seeking to monitor the state (what software is running) and activity of a home user's computer in order to protect digital content, the issue of remote attestation is far more problematic and has come, appropriately, under fire. In fact, one legislative effort to deputize this sort of private sector monitoring of private use of content and to privilege self-help by content companies was already vetted and rejected. Hopefully other systems that support remote access to consumers' computers will not introduce security holes, although developing systems that allow for remote access and control of networked PCs that cannot be exploited by a motivated attacker is likely a complicated task. Ross Anderson, 'Trusted Computing' Frequently Asked Questions, http://www.cl.cam.ac.uk/~rja14/tcpa-faq.html (last updated Aug. 2003); SCHOEN, *supra* note 158.

Existing law did not dissuade Sony BMG from introducing DRM-protected CDs that created security flaws. While it is almost certain that users had little to no idea that installing the XCP and MediaMax DRM would open security backdoors into their computers or allow remote monitoring of their activities and knowledge of their machine configuration, current EULA and contract law provides little hope for fixing the structure of either the consent process or the substantive terms of such contracts. As discussed *supra*, courts have shown little interest in examining all but the most egregious of contract terms and formation issues.

The need to consider the totality of the consumer contracting experience, rather than specific terms in isolation, suggests that successfully restructuring these interactions will require detailed fact finding about consumers' understandings and expectations, and the harms and risks to consumers and competition created by specific terms and consent procedures. Creating more nuanced and specific rules to govern consent with respect to software downloads is a task better undertaken by an administrative agency with deep expertise in consumer protection and the ability to provide guidance and forward-looking rules than by the courts. In the next Section, we consider the Federal Trade Commission's response to the flawed notice and consent provisions of Sony BMG's DRM and the privacy concerns to which they contributed.

C. Defining Deceptive and Unfair Acts: The Problem with Software Downloads and Privacy

At the time Sony BMG placed its DRM-protected CDs on the market, the FTC had already long demonstrated its authority to investigate and penalize parties making false statements about the collection, use, and disclosure of personal information.[240] In particular, successful enforcement

240. *See* Agreement Containing Consent Order, *In re* Sony BMG Music Entm't, FTC File No. 062 3019 (Jan. 30, 2007), *available at* http://www.ftc.gov/os/caselist/0623019/070130agreement0623019.pdf.

> [T]he disclosure shall be unavoidable and shall be presented prior to the consumer installing any content protection software or, if the disclosure is related to Internet connectivity, prior to causing any transmission to respondent about consumers, their computers, or their use of a covered product through Internet servers. The disclosure shall be of a size and shade, and shall appear on the screen for a duration, sufficient for an ordinary consumer to read and comprehend it. The disclosure shall be in understandable language and syntax.

Id. See FTC v. Seismic Entm't, Inc., No. 04-377, 2004 U.S. Dist. LEXIS 22788 (D.N.H. Oct. 21, 2004) (enjoining the unfair practice of exploiting a known vulnerability in the Internet Explorer web browser to download spyware to users' computers without their

actions were brought against companies, like Sony BMG, that offered public statements falsely disavowing the collection of information from users.[241] More recently, the FTC used its authority to bind companies to practices and procedures that provide a "reasonable" level of security for users' personal information.[242] Importantly, it successfully settled claims against companies for failing to implement practices to address commonly known and well-understood security vulnerabilities and for failing to identify and prevent security vulnerabilities that put customer information at risk.[243]

In light of these existing FTC actions, Sony BMG's inaccurate statements about data collection practices and software security, including vulnerabilities that could compromise personally identifiable information, appear inexplicable. However, a more careful consideration of the FTC's prior actions sheds some light on why Sony BMG may not have considered its practices objectionable as a matter of established FTC guidelines.

The centerpiece of the FTC's privacy enforcement actions has been the protection of individually identifiable personal information.[244] But, under

---

knowledge); *In re* Advertising.com, FTC File No. 042 3196 (Sept. 12, 2005). *See also* Complaint, FTC v. Odysseus Mktg., Inc., No. 05-CV-330 (D.N.H. Sept. 21, 2005) (failure to clearly and conspicuously disclose bundled software with security and privacy risks is deceptive).

241. *See* Microsoft Corp., 67 Fed. Reg. 52,723 (Fed. Trade Comm'n Aug. 13, 2002) (proposed consent order) (alleging that Passport misrepresented its data collection activities and obtaining consent order prohibiting such misrepresentations).

242. *See* MTS Inc., 69 Fed. Reg. 23,205 (Fed. Trade Comm'n Apr. 28, 2004) (proposed consent order) (failure to implement procedures that were reasonable and appropriate to detect and prevent "broken account and session management" vulnerabilities was unfair or deceptive given Tower Records's statements about attention to security and privacy); Eli Lilly & Co., 67 Fed. Reg. 4,963 (Fed. Trade Comm'n Feb. 1, 2002) (proposed consent order) (lack of proper controls to avoid disclosure of e-mail addresses was unfair or deceptive given statements to the contrary).

243. *See* Decision and Order, *In re* MTS, Inc., FTC File No. 032 3209 (May 28, 2004), *available at* http://www.ftc.gov/os/caselist/0323209/040602do0323209.pdf; Decision and Order, *In re* Guess?, Inc., FTC File No. 022 3260 (Aug. 5, 2003), *available at* http://www.ftc.gov/os/2003/08/guessdo.pdf; Decision and Order, *In re* Petco Animal Supplies, Inc., FTC File No. 032 3221 (Mar. 4, 2005), *available at* http://www.ftc.gov/os/caselist/0323221/050308do0323221.pdf; Agreement Containing Consent Order, *In re* BJ's Wholesale Club, Inc., FTC File No. 042 3160 (May 17, 2005), *available at* http://www.ftc.gov/os/caselist/0423160/050616agree0423160.pdf.

244. *See* Children's Online Privacy Protection Act of 1998, 15 U.S.C. § 6501 (2000).

> [Personal information means] individually identifiable information about an individual collected online including (a) a first and last name; (b) a home or other physical address including street name and name of a city or town; (c) an email address or other online contact information,

a literal reading of the FTC's application of that term, Sony BMG was not collecting "personal information." According to the FTC, the Sony BMG media player "establish[ed] a connection with Internet servers through which the user's or proxy server's Internet Protocol (IP) address and a numerical key identifying the album being played will be transmitted from the user's computer to the servers."[245] Such information was "used to display images and/or promotional messages on users' computers that are retrieved from those servers."[246] Under its only official statement on the issue, the FTC has said that "unless [IP addresses] are associated with other individually identifiable personal information, they would not fall within the . . . definition of 'personal information'" regulated by the Children's Online Privacy Protection Act.[247] Sony BMG's stance—that it collected no personal information that raised privacy concerns[248]—may seem counterintuitive, but viewed in light of the prevailing FTC definition of "personal information," Sony BMG's position becomes somewhat more coherent. While this in no way excuses the misleading statements found in

---

> including but not limited to an instant messaging user identifier, or a screen name that reveals an individual's email address; (d) a telephone number; (e) a social security number; (f) a persistent identifier, such as a customer number held in a cookie or a processor serial number, where such identifier is associated with individually identifiable information; or a combination of a last name or photograph of the individual with other information such that the combination permits physical or online contacting; or (g) information concerning the child or the parents of that child that the operator collects online from the child and combines with an identifier described in this definition.

Id.

See also FED. TRADE COMM'N, PRIVACY ONLINE: FAIR INFORMATION PRACTICES IN THE ELECTRONIC MARKETPLACE (2000), *available at* http://www.ftc.gov/reports/privacy2000/privacy2000.pdf (asking for legislation establishing rules, and providing the FTC with regulatory authority, to govern the commercial websites that collect "personal identifying information" from or about consumers).

245. Complaint, *In re* Sony BMG Music Enter., FTC File No. 062 3019, at para. 18 (Jan. 30, 2007), *available at* http://www.ftc.gov/os/caselist/0623019/070130cmp0623019.pdf.

246. *Id*.

247. FTC Children's Online Privacy Protection Rule, 16 C.F.R. § 312 (2006).

248. Carrie Kirby, *Sony Gets an Earful Over CD Software*, S.F. CHRON., Nov. 11, 2005, at A1; Jack Kapica, *CIPPIC Files Complaint Against SonyBMG Settlement*, GLOBEANDMAIL.COM, Sept. 21, 2006, http://www.theglobeandmail.com/servlet/story/RTGAM.20060921.gtsony0921/TPStory/Technology/columnists; Brian Garrity, *Sony BMG Agrees to DRM Settlement*, BILLBOARD, Jan. 7, 2006, at 5; Iain Thomson, *Sony BMG Settles Rootkit Lawsuit*, VNUNET.COM, Jan. 9, 2006, http://www.vnunet.com/vnunet/news/2148287/sony-settles-root-kit-fiasco.

Sony BMG's EULA, the narrow scope of the FTC's definition of personal information provides important context in which to consider Sony BMG's actions.

At the time Sony BMG put its DRM-protected CDs on the market, the FTC had already brought several actions—some pending and others successfully settled—against companies that had installed software without appropriate notice and consent procedures.[249] The majority of these cases involved "bundled software,"[250] where EULA disclosures were found insufficient to provide notice of the hidden software which typically served pop-up advertisements, collected click-stream data, or engaged in some other invasive data collection technique. Frequently the EULAs accompanying bundled software include multiple embedded or linked EULAs making the identification of the terms of the exchange complicated and time-consuming.

The software on the Sony BMG CDs, however, was not bundled in the traditional sense. Users did not intend to install some software but unknowingly install other software through the Sony BMG CD. Rather, most users likely did not intend to obtain any software at all during this interaction. Although the hidden and unexpected nature of the transactions at the root of the spyware-bundling cases provided a parallel to the Sony BMG CDs, Sony BMG may not have understood itself to be intentionally hiding the software in quite the same way as spyware companies.

---

249. FTC v. Seismic Entm't, Inc., No. 04-377, 2004 U.S. Dist. LEXIS 22788 (D.N.H. Oct. 21, 2004) (holding FTC was likely to succeed on the merits because it is an unfair practice to exploit a known vulnerability in the Internet Explorer web browser to download spyware to users' computers without their knowledge, and enjoining this method of software distribution); Analysis of Proposed Consent Order to Aid Public Comment, *In re* Advertising.com, FTC File No. 042 3196 (Aug. 3, 2005) (holding failure to clearly and conspicuously disclose bundled software that traced browsing deceptive); *see also* Complaint, FTC v. Odysseus Mktg., Inc., No. 05-CV-330 (D.N.H. Sept. 21, 2005) (alleging that failure to clearly and conspicuously disclose bundled software with security and privacy risks is deceptive).

250. In "bundled" software offerings, the user understands that they are installing one program, but because they fail to read the EULA, and the software attempts to hide itself in other ways, they fail to understand that they are in fact installing several different software programs and often creating relationships with several different companies. Typically these programs engage in invasive activities (pop-up or other forms of push advertising) or extractive activities (monitoring and data collection) that users presumably would avoid if given appropriate notice. *In re* Advertising.com, FTC File No. 042 3196 (Sept. 12, 2005) (holding failure to clearly and conspicuously disclose bundled software that traced browsing deceptive); *see also* Complaint, FTC v. Odysseus Mktg., Inc., No. 05-CV-330 (D.N.H. Sept. 21, 2005) (holding that failure to clearly and conspicuously disclose bundled software with security and privacy risks is deceptive).

In contrast to the bundled spyware cases, Sony BMG was installing only one piece of software and using a single EULA, which was, in form, consistent with the standard industry practice. The combination of standard disclosure through a EULA and the collection of no "personal information" may have led Sony BMG to conclude that their installation and data collection procedures were consistent with the law and industry norms. This may have been further buttressed by the failure of surveillance law generally to set limits on surreptitious monitoring and data collection in the context of advertising and commercial dealings as long as such monitoring is disclosed in the EULA.[251]

In the Sony BMG consent order, the FTC provided a new twist to the existing privacy landscape. The order stands for the propositions that: (i) clear and prominent notice and consent is required on CDs that condition access to content on the installation of software that monitors and reports on user activities; and (ii) clear and prominent notice and consent is required, again, before information about users, their computers, or their use of the CD's content is transmitted.[252] Through the Sony BMG order and bundled spyware orders, the FTC has established that software that collects and transmits information about users, their computers, or their use of the content—even if not "personal information" under the COPPA definition—raises privacy concerns.[253] The Sony BMG order also creates a requirement, at least with respect to Sony BMG, that the installation of software from a CD, and the transfer of information by such software, re-

---

251. Patricia L. Bellia, *Spyware and the Limits of Surveillance Law*, 20 BERKELEY TECH. L.J. 1283, 1306-11 (2005) (discussing courts' general willingness to allow consent to interception to be given through "click-wrap" EULA provisions and therefore limiting the utility of Wire Tap Act and Computer Fraud and Abuse Act to provide remedies to a large set of spyware problems).

252. Agreement Containing Consent Order, *In re* Sony BMG Music Entm't, FTC File No. 062 3019 (Jan. 30, 2007), *available at* http://www.ftc.gov/os/caselist/0623019/070130agreement0623019.pdf

253. Where collection and transmission is part of the standard operation of internet protocols, clearly this cannot be the case. This line, which we are identifying, but is not clearly established in the settlements, may be a hard one to identify and maintain. In the context of traditional web-based interactions, IP addresses are routinely disclosed to the servers from which a user is requesting content (a web page, for example). In this context the requirement that notice and consent occur seems inappropriate. The Sony BMG phone-home feature is the opposite end of the spectrum, in that there is no need for users' machines to interact with Sony BMG's servers. There are many areas in between, and as technology changes, what is necessary and expected will likely change with it.

quires heightened "clear and prominent"[254] notice and consent.[255] Interestingly, the order does not create an obligation to analyze the security properties of products before release. Such obligations are found in earlier FTC orders and the absence here is noteworthy, particularly given that a provision of Sony BMG's settlement with the Attorney Generals requires that at least one qualified, independent third-party expert review future content protection software and conclude that it creates no "confirmed security vulnerabilities" prior to use by Sony BMG.[256]

Like the security vulnerability at issue in prior FTC actions, rootkits and privilege escalation are known, dangerous security vulnerabilities. However several factors make the Sony BMG system distinct, and distinctly troubling. As discussed *supra* in Part II, it seems likely that the choices to design and deploy software with these security vulnerabilities were deliberate and intentional design decisions, not failures of otherwise secure software or loopholes left unaddressed despite a security-conscious design process. Reflecting these distinctions, the FTC complaint against Sony BMG and, to some extent, the final order, included an unfairness claim based on the installation of the security vulnerabilities and the lack of adequate notice and consent during installation in addition to deception claims based on the affirmatively misleading omissions of material facts.

The unfairness claim is the most important element of the order because unfairness does not rely upon the content or sufficiency of statements made to the public, but rather evaluates the substantive impact of

---

254. *See* Agreement Containing Consent Order, *In re* Sony BMG Music Entm't, FTC File No. 062 3019 (Jan. 30, 2007), *available at* http://www.ftc.gov/os/caselist/0623019/070130agreement0623019.pdf

> [T]he disclosure shall be unavoidable and shall be presented prior to the consumer installing any content protection software or, if the disclosure is related to Internet connectivity, prior to causing any transmission to respondent about consumers, their computers, or their use of a covered product through Internet servers. The disclosure shall be of a size and shade, and shall appear on the screen for a duration, sufficient for an ordinary consumer to read and comprehend it. The disclosure shall be in understandable language and syntax.

Id.

255. *See id.* (prohibiting downloads unless a consumer "dictates his/her assent to install such software by clicking on a button or link that is clearly labeled or otherwise clearly represented to convey that it will activate the installation, or by taking a substantially similar action").

256. Settlement Agreement at 27, *In re* Sony BMG CD Techs. Litig., No. 1:05-CV-09575 (S.D.N.Y. Dec. 28. 2005), *available at* http://www.eff.org/IP/DRM/Sony-BMG/sony_settlement.pdf.

the businesses activity itself. In this way it is akin to substantive unconscionability in contract law. The FTC found that Sony BMG's installation practices and security vulnerabilities caused substantial injury that users could not reasonably avoid and were not outweighed by any countervailing interests.[257]

The Sony BMG order set two important new baselines. First, the complaint and ensuing order make clear that certain software may not be installed on a user's computer regardless of the consent experience.[258] In particular it prohibits the installation of content protection software that hides, cloaks or misnames files, folders, or directories, or misrepresents the purpose or effect of files, directory folders, formats, or registry entries.[259] This effectively prohibits the installation of content protection software that uses a rootkit like the one contained in XCP. While the order does not explicitly prohibit software that alters system, directory, or file privileges, such as MediaMax, it does require that such software be fairly represented to the consumer both through disclosures during installation and appropriate naming conventions.[260]

Second, where limits are placed on the expected functionality of a CD or information about the consumers' use of the CD is to be transferred, the user must receive clear and prominent notice and must communicate assent affirmatively.[261] This extends to information beyond the personally identifiable information traditionally at the heart of the FTC's privacy initiatives and enforcement actions. The first of these provisions is significant because it begins to establish an obligation to provide heightened notice aimed at truly informing consumers of material changes to functionality of media containing copyrighted works. The second is significant be-

---

257. *See* Agreement Containing Consent Order, *In re* Sony BMG Music Entm't, FTC File No. 062 3019 (Jan. 30, 2007), *available at* http://www.ftc.gov/os/caselist/0623019/070130agreement0623019.pdf.

258. *Id.* at 6.

259. *Id.*

> [Software] shall not install or cause to be installed on a consumer's computer any content protection software that prevents the consumer from readily locating or removing the software, including but not limited to by: (1) hiding or cloaking files, folders, or directories; (2) using random or misleading names for files, folders, or directories; or (3) misrepresenting the purpose or effect of files, directory folders, formats, or registry entries.

Id.

260. *Id.*

261. *Id.*

cause it recognizes a privacy interest in surveillance separate from the focus of prior FTC activity dealing with personally identifiable information.

The FTC and state Attorneys General settlements in the Sony BMG matter are a testament to the power of broad and flexible grants of authority that provide a basis for tailoring responses to new marketplace practices that mislead or injure consumers and materially disrupt settled consumer expectations. But at the same time, the fact that a large, reputable company of Sony BMG's stature was likely unaware that it was acting deceptively or unfairly highlights the problems the FTC and state Attorneys General face in attempting to endorse and enforce marketplace practices that promote meaningful contracting in the online environment. Given the judiciary's unwillingness to set limits or boundaries on the formalities or substance of contracting, this is a particularly daunting task.[262] A case-by-case approach, whether undertaken in agencies or courts, fails to provide clear guidance to companies seeking to engage fairly with consumers and allows ample room for companies to use EULAs to obtain "consent" to overreaching and egregious practices that are inconsistent with consumer expectations or that pose harm. The ongoing struggle within industry to define self-regulatory rules to distinguish legitimate software and business practices from spyware, as well as the ever-growing legislative efforts to address spyware, are a tribute to the yawning grey zone confronting both businesses and consumers and the inadequacy of current contract law to assist in their navigation.

VI. REALIGNING SKEWED INCENTIVES

Having traced the constraints and influences that encouraged and permitted Sony BMG to deploy its DRM strategy, this Part offers potential reforms, both legal and technical, aimed at reshaping the system of incentives that gave rise to the rootkit incident to guard against future harm to the public and the network. First, we build upon the Copyright Office's most recent DMCA rulemaking and suggest a permanent statutory exemption that enables researchers and lay users to proactively identify and remove dangerous protection measures from their systems. Second, we look to insights drawn from the field of HCI-Sec as an additional foundation for the development of more effective notice and consent guidelines and standards governing software downloads and online data collection practices. We argue that the FTC is the best situated institution for incorporating in-

262. Copyright Protection and Management Systems, 17 U.S.C. § 1201(a)(1)(C).

terdisciplinary insights, such as HCI-Sec, in developing such guidelines and standards.

But before outlining these recommendations, two antithetical but equally misguided reactions to the rootkit incident should be addressed. First, a superficial overview of the rootkit incident may suggest—and some will certainly argue—that no response is necessary. Sony BMG, the argument will go, miscalculated the tradeoff between preventing infringement and protecting user security, as a matter of both law and marketing. The investigations, lawsuits, and settlements that came in the wake of XCP and MediaMax simply demonstrate that the corrective mechanisms already in place served their function by holding Sony BMG accountable for its socially harmful behavior. The public flogging Sony BMG received from the press, consumer advocate groups, state Attorneys General, and the FTC will stand as a warning to other content owners and DRM vendors to behave more responsibly in the future.

Although it is undoubtedly true that no record label is likely to introduce protection measures that install rootkits on their customers' computers anytime soon, the ways in which privacy and security can be compromised by DRM are numerous. So long as the system of incentives that produced the rootkit incident remains in place, we can expect further abuses in the future. Although "rootkit" remains a watchword in the world of content protection, institutional memories—much like public awareness—will fade. Rather than relying solely on the content industry's insistence that it has learned its lesson, responsible public policy requires institutional reforms that recognize and counteract the lure of overzealous DRM implementation. Moreover, the anti-interventionist position fails to account for the importance of public interest advocates, the press, and public outcry in pressuring Sony BMG to settle the legal claims brought against it. Such a fortuitous feedback loop cannot be guaranteed in the future, and the protection of end user and network security should not hinge on something as rare and unpredictable as the perfect storm.

Second, standing in stark contrast to this hands-off approach is one that calls for prohibitions on particular technologies in the name of consumer protection. But the rootkit incident should not be understood to make a case for legislation that mandates or prohibits particular technological design decisions. In an extreme form, such legislation could ban the use of rootkits—or even DRM—altogether.[263] This response is mis-

263. Although the FTC's Sony BMG order prohibited Sony BMG from using any content protection software that incorporates a rootkit or similar technology, this is a far

guided for a number of reasons. Both rootkits and DRM can, in some instances, serve useful and legitimate purposes. DRM can enable new business models, such as digital video "rental," that as a matter of economics would prove impossible without some enforcement mechanism for use restrictions.[264] Likewise, legitimate software developers, such as anti-virus vendors, have used rootkits to protect their programs from attack.[265]

While not as pernicious as technological mandates, prohibitions against particular software tools could set dangerous legislative precedent. As a matter of institutional competence, legislators are poorly positioned to insert themselves into the design decisions of technology developers. Congress, in drafting the DMCA, recognized the bounds of its expertise as well as the risks to innovation posed by governmental interference in the minutiae of software and product design.[266] Rather than the immediate constraints on design alternatives that would result from a technological mandate, banning particular software or product components could give rise to a legislative incrementalism that in time will yield the same unfortunate result.

Aside from being dangerous, this tack would also prove ineffective. In all likelihood, rootkits will not prove the next serious threat to end user security and privacy. Legislative or regulatory efforts that narrowly target specific technologies will almost always come a day too late to provide meaningful protection for consumers and network resources.[267] Rather

---

cry from generally applicable legislation that constrains all technology developers and all potential products. *See* Agreement Containing Consent Order, *In re* Sony BMG Music Entm't, FTC File No. 062 3019 (Jan. 30, 2007), *available at* http://www.ftc.gov/os/caselist/0623019/ 070130agreement0623019.pdf.

264. Whether the enforcement mechanism requires or deserves the benefit of legislation like the DMCA to introduce the force of law as an additional layer of enforcement is analytically distinct from the technology's importance to new business models.

265. This decision stirred controversy. *See supra* note 2.

266. Copyright Protection and Management Systems, 17 U.S.C. § 1201(c)(3).

> (3) Nothing in this section shall require that the design of, or design and selection of parts and components for, a consumer electronics, telecommunications, or computing product provide for a response to any particular technological measure, so long as such part or component, or the product in which such part or component is integrated, does not otherwise fall within the prohibitions of subsection (a)(2) or (b)(1).

Id.

267. Stefanie Olsen, *Nearly Undetectable Tracking Device Raises Concern*, CNET NEWS.COM, July 12, 2000, http://news.com.com/2100-1017-243077.html; Posting of Peter Fleisher to The Official Google Blog, http://googleblog.blogspot.com/2007/07/cookies-expiring-sooner-to-improve.html (July 16, 2007 09:52 PST); BRUCE H. KOBAYASHI & LARRY E. RIBSTEIN, A RECIPE FOR COOKIES: STATE REGULATION OF CONSUMER

than seeking to prevent a carbon copy of the most recent disaster, any useful response must attempt to reform the underlying factors that spur content owners to adopt dangerous DRM.

A. Enabling Security Research and Self-Help Through a Statutory Exemption to the DMCA

As described *supra*, the DMCA, by discouraging security research and criminalizing the distribution of software tools that enable users to protect themselves from harmful DRM, served as a key component of the legal landscape that permitted the rootkit debacle.[268] By establishing a permanent statutory exemption from DMCA liability, Congress could take a significant step towards preventing future threats to end user and network security.

In drafting the DMCA, Congress recognized the need to respond to changing circumstances given the fluidity of the nascent environment it sought to prospectively regulate and the otherwise lawful uses that might be adversely affected by the broad prohibition on circumvention. To retain some flexibility, Congress created a rulemaking proceeding that serves as a "fail-safe mechanism" intended to ensure that limits on the prohibition on circumvention keep pace with developments in the market for copyrighted works.[269] This proceeding requires the Librarian of Congress, acting on the recommendation of the Register of Copyrights, to conduct a rulemaking hearing to identify classes of copyrighted works the noninfringing uses of which are likely to be adversely affected by the prohibition on circumvention in the succeeding three year period.[270] Users of copyrighted works that fall within exempt classes are not subject to the prohibition against circumvention.[271]

MARKETING INFORMATION (2001), http://www.law.gmu.edu/faculty/papers/docs/ 01-04.pdf.

268. *See supra* Section V.A.

269. H.R. REP. NO. 105-551, pt. 2, at 35 (1998). As the Report explained, "The primary goal of the rulemaking proceeding is to assess whether the prevalence of these technological protections, with respect to particular categories of copyrighted materials, is diminishing the ability of individuals to use these works in ways that are otherwise lawful." *Id.* at 37.

270. *See* § 1201(a)(1)(C). For a detailed discussion and overview of the DMCA rulemaking process, the exemptions granted in 2006, and the limitations of this process in providing adequate protection to the public, *see generally* Aaron Perzanowski, *Evolving Standards and the Future of the DMCA Anticircumvention Rulemaking*, 10 J. OF INTERNET L., Apr. 2007, at 1.

271. 17 U.S.C. § 1201(a)(1)(B) (2000).

In 2006, the Copyright Office recommended, and the Librarian of Congress granted, an exemption requested by the Samuelson Law, Technology & Public Policy Clinic of the University of California, Berkeley School of Law, on behalf of Felten and Halderman[272] that permits the circumvention of technological protection measures distributed on audio CDs when those measures create or exploit vulnerabilities that compromise the security of personal computers.[273] This exemption, crafted to closely track the facts of the rootkit incident in light of the Copyright Office's traditionally conservative attitude toward the granting of exemption proposals,[274] offers meaningful protection to both lay users and researchers who seek to eliminate security vulnerabilities introduced by DRM on audio CDs. Prior to the exemption, genuine legal uncertainty existed as to whether a user who unknowingly installed XCP could be held liable under the DMCA for its removal or whether a researcher who bypassed the DRM in an effort to discern its operation violated section 1201.[275]

---

272. *See generally* Comment of Edward W. Felten & J. Alex Halderman to the United States Copyright Office, *supra* note 89.

273. Exemption to Prohibition on Circumvention of Copyright Protection Systems for Access Control Technologies, 71 Fed. Reg. 68,472 (Nov. 27, 2006) (to be codified at 37 C.F.R. § 201.40), *available at* http://www.copyright.gov/fedreg/2006/71fr68472.html; Memorandum from Marybeth Peters, Register of Copyrights, United States Copyright Office, to James H. Billington, Librarian of Congress, concerning Rulemaking on Exemptions from Prohibition on Circumvention of Copyright Protection Systems for Access Control Technologies (Nov. 17, 2006), *available at* http://www.copyright.gov/1201/docs/1201_recommendation.pdf.

274. Somewhat surprisingly, the Copyright Office revisited the standards for the DMCA Rulemaking in 2006, potentially opening the door for an increase in narrowly tailored exemptions. *See* Perzanowski, *supra* note 270, at 19-20.

275. In something of an ironic turn, copyright industry representatives sought to defeat the exemption by claiming that: (i) the protection measures used on CDs were copy controls rather than access controls, and thus outside the scope of the anti-circumvention provisions; (ii) existing statutory exemptions, most notably the security testing exemption of section 1201(j), rendered an exemption unnecessary; and (iii) Sony BMG's voluntary release of a tool to uninstall the rootkit obviated the need for an exemption. *See generally* Testimony of Steven Metalitz, http://www.copyright.gov/1201/2006/hearings/transcript-mar31.pdf; Joint Reply Comment, http://www.copyright.gov/1201/2006/reply/11metalitz_AAP.pdf. Rejecting these arguments, the Register concluded that because particular software was required to play a CD on a computer, the technical protection measure used in the DRM at issue was an access control. Memorandum from Marybeth Peters, *supra* note 273, at 56. Because the scope of section 1201(j)—a provision not yet meaningfully interpreted by the courts—was ambiguous, the Register concluded that consideration of the exemption on its merits was appropriate. In light of the need for researchers to identify security vulnerabilities created by CD protection measures, the dangers posed by such measures to consumers, the unclear potential liability under the DMCA, and the

However, the new exemption and the rulemaking procedure itself are insufficient tools to address the security risks posed by technological protection measures. First, the exemption is temporary, with an expiration date of October 2009.[276] Second, the exemption applies only to the extent circumvention occurs for the sole purpose of good faith testing, investigating, or correcting security vulnerabilities, leaving some risk that those who also hope to place music on their iPods after eliminating the security threats could face liability.[277] Third, the exemption is limited to a particular medium—the Compact Disc—and a particular type of work—sound recordings. While these limitations were necessary as a practical matter to secure the endorsement of the Register of Copyrights, they are by no means ideal from a policy perspective. Protection measures that create security vulnerabilities could be introduced in a multitude of media in connection with any type of copyrighted work. As discussed *supra*, a solution tied to the specific facts of yesterday's disaster fails to account for variations on the theme.

But from a practical standpoint, by far the most fundamental inadequacy of the DMCA rulemaking is inherent in the Copyright Office's statutory authority. The rulemaking can exempt certain classes of works from the anti-circumvention provision, but Congress vested no authority in the Copyright Office or Librarian of Congress to grant corresponding exemptions from the anti-trafficking provisions.[278] This asymmetry gives rise to a rather perverse result: an act of circumvention is permitted by an exemption, but the tools necessary to take advantage of that privileged use

---

resulting adverse impact on the ability to engage in noninfringing uses, the Register recommended adoption of the exemption. *Id.*

276. Exemption to Prohibition on Circumvention of Copyright Protection Systems for Access Control Technologies, 71 Fed. Reg. at 68,472, *available at* http://www.copyright.gov/fedreg/2006/71fr68472.html. Maintaining the exemption will require proof of ongoing harm during the next rulemaking. Broadening it to cover additional technological protection measures found to present security risks will require separate showings of ongoing harm to a class of works. Given the fallout over the Sony BMG DRM, it is possible that no protection measures that create security risks will be released on CDs in the coming three years, making it impossible to renew the exemption. While this will mean that no security-flaw-riddled DRM is on the marketplace, it will also remove an important incentive for copyright holders to ensure the safety of their protection measures going forward. *See* Perzanowski, *supra* note 270.

277. Exemption to Prohibition on Circumvention of Copyright Protection Systems for Access Control Technologies, 71 Fed. Reg. at 68,472, *available at* http://www.copyright.gov/fedreg/2006/71fr68472.html.

278. Copyright Protection and Management Systems, 17 U.S.C. § 1201(a)(1)(C).

remain illegal.[279] Thus although both the public and security researchers may engage in circumvention under the new exemption, researchers like Felten and Halderman could still face potential liability for distributing tools to assist the public in exercising this exemption. Given that the average CD purchaser will possess neither the knowledge nor ability to eliminate the security risks of a protection measure without a software tool, the inability of the exemption process to free experts to develop tools renders this new right much less meaningful.

The solution to the shortcomings of the DMCA rulemaking must be a legislative one.[280] But rather than simply extend the authority of the Copyright Office to include the power to exempt classes of works from the DMCA's anti-trafficking provisions as well—a development the authors would welcome—Congress should simply expand the existing permanent statutory exemption found in section 1201(j) to permit both circumvention and trafficking to the extent undertaken to investigate or eliminate protection measures that "create or exploit security flaws or vulnerabilities that compromise the security of personal computers."[281]

B. Developing Meaningful Notice and Consent Mechanisms through Interdisciplinary Insight and Agency Action

As discussed *supra*, the security vulnerabilities in the DRM Sony BMG deployed are best viewed as intentional design choices. While Sony BMG is responsible for deploying dangerous software, the ease with which the software could be surreptitiously installed on consumers' ma-

279. The "reverse notice and takedown" process put forward by Reichman, Dinwoodie, and Samuelson in this volume proposes to address the limited technical ability of the general public by requiring copyright owners to take down technical protections to make tools for "public good" uses. Jerome H. Reichman, Graeme B. Dinwoodie, & Pamela Samuelson, *A Reverse Notice and Takedown Regime to Enable Public Interest Uses of Technically Protected Copyrighted Works*, 22 BERKELEY TECH. L.J. 981 (2007). This innovative approach would instill some needed balance back into the DMCA; however, it will not create room for research on protection measures themselves, nor create a safe harbor for those who create tools to enable users to make public good uses. *Id.*

280. Representatives Rick Boucher and John Doolittle's Freedom And Innovation Revitalizing U.S. Entrepreneurship Act would enshrine the current temporary exemptions and add additional valuable permanent exemptions; it does not, however, address the unnecessarily narrow scope of the "rootkit" exemption. H.R. 1201, 110th Cong. (2007). The authors humbly suggest that the bill would benefit from incorporation of the recommendations contained in this section.

281. Currently section 1201(j) applies only to (a)(1) and (a)(2). 17 U.S.C. § 1201(j) (2000). In light of the tortured distinction between copy controls and access controls, its scope should be expanded to include section 1201(b) as well.

chines causes us to reflect on the state of consumer control over the activities—software downloads and data collection and transmission—occurring on their desktops more generally. Consumer protection law has an important role to play in reforming the notice and consent process with respect to software installation and data collection practices.

But we believe that innovative reforms in this area will come about from a broader interdisciplinary approach. The FTC decisions discussed *supra*, in Section V.C, begin to chart a course in this direction. Incorporating insight from the field of HCI-Sec would enable the FTC and other consumer protection agencies to craft guidelines for language and mechanisms to facilitate effective notice and informed consent. Such guidelines would vest consumers with increased control of the software downloaded onto their machines and the information collected and transmitted about their activities.

A growing team of HCI-Sec researchers is exploring "usable privacy and security."[282] The Sony BMG disaster is one in a string of examples of the difficulties facing computer users in making good security and privacy choices about their computing environment.[283] It is imperative that users understand, value, and implement security. The question under exploration

---

282. See HCISec Bibliography, http://www.gaudior.net/alma/biblio.html, for an up-to-date list of contributions in this field. With respect to privacy, HCISec practitioners have studied a variety of fields. For research on browsers, see, for example, Batya Friedman, Daniel C. Howe, & Edward Felten, *Informed Consent in the Mozilla Browser: Implementing Value-Sensitive Design*, *in* PROCEEDINGS OF THE THIRTY-FIFTH ANNUAL HAWAI'I INTERNATIONAL CONFERENCE ON SYSTEM SCIENCES; Umesh Shankar & Chris Karlof, *Doppelganger: Better Browser Privacy Without the Bother*, *in* THIRTEENTH ACM CONFERENCE ON COMPUTER AND COMMUNICATIONS SECURITY (2006); for peer-to-peer file-sharing research, see, for example, Nathaniel S. Good & Aaron Krekelberg, *Usability and Privacy: A Study of Kazaa P2P File-Sharing*, *in* PROCEEDINGS OF THE ACM CONFERENCE ON HUMAN FACTORS IN COMPUTING SYSTEMS (CHI 2003); for notices and spyware acquisition, see, for example, Mulligan et al., *supra* note 234; for operating system research, see, for example, Alex J. DeWitt & Jasna Kuljis, *Aligning Usability And Security—A Usability Study Of Polaris*, *in* PROCEEDINGS OF THE 2006 SYMPOSIUM ON USABLE PRIVACY AND SECURITY 12-14 (2006); and for phishing, see, for example, Rachna Dhamija & J.D. Tygar, *The Battle Against Phishing: Dynamic Security Skins*, SYMPOSIUM ON USABLE PRIVACY AND SECURITY (2005); Rachna Dhamija, J.D. Tygar, & Marti Hearst, *Why Phishing Works*, *in* PROCEEDINGS OF THE SIGCHI CONFERENCE ON HUMAN FACTORS IN COMPUTING SYSTEMS (2006).

283. *See* A. Herzog et al., *User Help Techniques for Usable Security*, PROCEEDINGS OF THE 2007 SYMPOSIUM ON COMPUTER HUMAN INTERACTION FOR THE MANAGEMENT OF INFORMATION TECHNOLOGY, Article No. 11 (2007) (discussing research revealing that inadequate usability results in security failures in many contexts including firewalls, Internet Explorer, Word, Outlook Express, encrypting email clients, and login systems).

in the HCI-Sec community, and directly relevant to the consumer protection mandate of the FTC and related agencies, is how to make privacy and security compelling, usable, and routine to end-users.

One problem with current user interface design is that users do not play a central role in controlling their security and privacy choices. Anti-virus and anti-spyware vendors have stepped in to assist users in maintaining a safe computing environment, but reliance on third-party vendors for defense is insufficient due to the contextual, process-based nature of both privacy and security.[284] For example, the same program functionality can have radically different consequences depending upon the context—compare a parent's installation of a program to create a safe online experience for a child to a similar program installed by a third party on the machine of an unconsenting adult. Given that users' opinions about the desirability of particular functionalities may be dramatically altered by the context of its intended use, effective privacy and security management must allow users to play a central role in controlling their privacy and security profiles. Because of this contextual variation of the value of privacy and security tools, techniques that fail to account for user autonomy are unworkable, even if the current state of desktop security and privacy tools is beyond the grasp of the average user.[285]

The failure of consumers to appropriately respond to disclosures of the privacy and security features of their products poses another problem. Research in HCI-Sec and related fields finds that information about a product's functionality, even when fully and accurately disclosed, often fails to capture the attention of computer users or to aid them in acting in a man-

---

284. By "contextual", we mean that decisions about information flow and access, integral to utilizing both privacy and security, tend to be context-dependent rather than absolute, i.e., individuals' concerns may vary widely depending upon the nature of perceived risks, which is related to the information or activity to be protected and the parties involved. For an exploration of the contextual nature of privacy, see Helen Nissenbaum, *Privacy as Contextual Integrity*, 79 WASH. L. REV. 119 (2004). By "process-based", we mean that providing security and privacy requires an ongoing evaluation of emerging threats, changing resources of adversaries, and changes in technology. One cannot adopt a policy to protect either at a given point in time and consider protection complete.

285. The remainder of this section primarily explores mechanisms for engaging users in effective decision-making. Another common approach to security is to build it in and automate it to the extent possible. These techniques are not mutually exclusive, but reflect differences in orientation to system design, the first being user-centric, the second being security- and system-centric. *See* Ka-Ping Yee, *User Interaction Design for Secure Systems*, *in* PROCEEDINGS OF THE 4TH INTERNATIONAL CONFERENCE ON INFORMATION AND COMMUNICATIONS SECURITY (LECTURE NOTES IN COMPUTER SCIENCE 2513), 278-290 (2002); Herzog et al., *supra* note 283.

ner consistent with their stated interests.[286] If the legal framework is to actually aid consumers in marketplace transactions, a primary goal of consumer protection agencies should be making security and privacy "usable."

A number of barriers hinder efforts to engage users in privacy and security decision-making.[287] First, security is typically a secondary concern undertaken in support of some other objective.[288] Second, there is little time or tolerance for trial and error in security decision-making, as decisions must be correct the first time.[289] Third, experimental research demonstrates that users' stated privacy preferences do not always align with their behavior[290] and that during task completion users will put off privacy or security protective behaviors.[291] Fourth, cognitive biases lead individuals to discount future privacy or security losses if presented with an immediate benefit,[292] reinforcing all of the above. These barriers combine with more generic problems, identified in the context of notice design generally,[293] to create a very difficult problem and design space.

Building upon the usability metrics of effectiveness, efficiency, and satisfaction,[294] HCI-Sec researchers have developed guidelines for align-

---

286. Good et al., *supra* note 234; Mulligan et al., *supra* note 234 (concluding in part that users' failure to delve into documentation describing software functionality stems from the incomprehensible nature of the EULAs that typically house these disclosures).

287. Much of the discussion below draws on work on either security or privacy, and in a few instances both. For the points we are highlighting, we believe that the research on privacy and security can be generalized across the two topics.

288. Herzog et al., *supra* note 283; J. Hardee et al., *To Download or not to Download: An Examination of Computer Security Decision Making*, INTERACTIONS (May & June 2006), at 32.

289. Herzog et al., *supra* note 283.

290. Hardee et al., *supra* note 288.

291. *Id.*

292. Acquisti & Grossklags, *supra* note 103.

293. HCI researchers are studying the effects of notification systems in computing generally, in particular focusing on cognitive response to interruptions. Notification systems often use visualization or auditory techniques to simply convey information with minimal distraction from primary tasks. A broad range of research has examined the creation of effective notice systems that limit the chances of warnings being dismissed or ignored. *See* E. Cutrell, M. Czerwinski, & E. Horvitz, *Notification, Disruption and Memory: Effects of Messaging Interruptions on Memory and Performance*, *in* HUMAN-COMPUTER INTERACTION: INTERACT '01 263 (Michitaka Hirose ed. 2001), *available at* http://research.microsoft.com/~cutrell/interact2001messaging.pdf.

294. ISO standard 9241-11 defines usability as the "[e]xtent to which a product can be used by specified users to achieve specified goals with effectiveness, efficiency and satisfaction in a specified context of use." "Effectiveness is defined as the accuracy and

ing security and usability,[295] as well as an approach that recognizes the importance of user autonomy in framing security considerations.[296] Using the guidelines and methodologies of HCI-Sec to analyze the design of

---

completeness with which users achieve specified goals." "Efficiency is measured by relating the level of effectiveness achieved to the resources used." "Satisfaction (defined as freedom from discomfort and positive attitudes to the use of the product) is a response of users to interaction with the product." *See* Halderman & Felten, *supra* note 11.

295. Yee, *supra* note 285.

> *Path of Least Resistance.* The most natural way to do any task should also be the most secure way.
>
> *Appropriate Boundaries.* The interface should expose, and the system should enforce, distinctions between objects and between actions along boundaries that matter to the user.
>
> *Explicit Authorization.* A user's authorities must only be provided to other actors as a result of an explicit user action that is understood to imply granting.
>
> *Visibility.* The interface should allow the user to easily review any active actors and authority relationships that would affect security-relevant decisions.
>
> *Revocability.* The interface should allow the user to easily revoke authorities that the user has granted, wherever revocation is possible.
>
> *Expected Ability.* The interface must not give the user the impression that it is possible to do something that cannot actually be done.
>
> *Trusted Path.* The interface must provide an unspoofable and faithful communication channel between the user and any entity trusted to manipulate authorities on the user's behalf.
>
> *Identifiability.* The interface should enforce that distinct objects and distinct actions have unspoofably identifiable and distinguishable representations.
>
> *Expressiveness.* The interface should provide enough expressive power (a) to describe a safe security policy without undue difficulty; and (b) to allow users to express security policies in terms that fit their goals.
>
> *Clarity.* The effect of any security-relevant action must be clearly apparent to the user before the action is taken.

Id. Saltzer and Schroeder also suggest:

> [*Least privilege.*] Every program and every user of the system should operate using the least set of privileges necessary to complete the job.

J. H. Saltzer & M. D. Schroeder, *The Protection of Information in Computer Systems*, *in* 63-9 PROCEEDINGS OF THE IEEE, 1278, *available at* http://web.mit.edu/Saltzer/www/publications/protection/.

See also D. Balfanz, D.K. Smetters, & R. Grinter, *In Search of Usable Security: Five Lessons from the Field*, IEEE SECURITY & PRIVACY (Sept.-Oct. 2004), at 19; I. Flechais, A.M. Sasse, & S.M.V. Hailes, *Bringing Security Home: A Process For Developing Secure and Usable Systems*, *in* WORKSHOP ON NEW SECURITY PARADIGMS 49 (2003).

296. Yee, *supra* note 285.

AutoRun identifies core ways in which its design facilitated, or at least failed to prevent, Sony BMG's behavior.

The process of software installation under the default configurations of AutoRun violated several HCI-Sec usable security principles.[297] First, the principle of *explicit authorization* requires that delegations of authority require explicit user action that is actually understood by the user as an act of delegation. The decision of what software is on a machine is generally a decision for users.[298] By allowing others to install software without providing users with notice and the ability to affirmatively delegate or withhold the privilege of doing so, AutoRun ran afoul of this design principle. The failure of AutoRun to expose the action of downloading to the user in a meaningful manner ran afoul of the *visibility* principle as well. *Visibility* requires the interface to represent, in an easily understandable manner, all active actors and authority relationships (who can take what action amongst actors or on resources) that would affect security-relevant decisions.[299] The pop-up security notices produced by AutoRun did not achieve the level of *expressiveness* sufficient to describe a safe security policy and allow users to choose among security options.[300] In addition, the effect of installing the DRM software on the security of the users' system was not apparent to the users either before, during, or after installation. This violates the *clarity* principle.[301] Finally, the rootkit violated the principle of *revocability* by making it exceedingly difficult for the user to revoke her delegation.[302]

The HCI-Sec principles of explicit authorization, visibility, expressiveness, clarity, and revocability are reflected to some extent in the FTC Sony BMG order which directs more forthright communication with users and greater affirmative control over the installation of software and the collection and transmission of data. Through enforcement actions against spyware distributors, the Federal Trade Commission and state Attorneys

297. For the purpose of this analysis we use the principles set forth in Yee, *supra* note 285. They are more inclusive and detailed that those found in other discussions of this subject. For several case studies on usability and security and additional insight into integrating them into the design process, *see* HCISec Bibliography, *supra* note 282.

298. Yee, *supra* note 285. In the context of an employer-employee relationship, the employer often makes decisions about computer configuration and software.

299. *See id.*

300. *Id. See also* Herzog et al., *supra* note 283 (critiquing "security by pop-up windows" based on research that shows it leads users to click through to return to the first order task).

301. *Id.*

302. *Id.*

General have begun to establish what are likely to become de facto policies limiting the reliance on EULAs as a means of adequate disclosure with respect to spyware programs, and perhaps other downloadable software. The consent orders and judgments establish a new form of consent, "express consent," which must be obtained prior to the installation, separate and apart from the EULA.

The efforts of HCI-Sec researchers are buttressed by efforts in the private sector to establish best practices for the notice and consent experience mechanism in response to the growing problems with spyware.[303] The Antispyware Coalition, a group of anti-spyware software companies, academics, and consumer groups building consensus about definitions and best practices in the debate surrounding spyware and other potentially unwanted technologies, similarly concluded that "EULAs alone are usually not enough to offset risk behaviors." Just as "express consent" as defined by the FTC and state Attorneys General requires "clear and prominent" disclosures, the Coalition's best practices require "clear and prominent" disclosures to be unavoidable and accessible (language, presentation, size) to "an ordinary consumer." They also establish heightened demands for communicating assent, requiring that software installations are clearly indicated on the button or other user interface that activates them.[304] In addition, these agreements begin to constrain the bundling of spyware and adware software with "free" programs to deceive consumers, and set procedural and substantive rules about uninstall procedures.[305]

---

303. ANTI-SPYWARE COALITION, *supra* note 185 ("For potentially unwanted technologies, EULAs alone are usually not enough to offset risk behaviors. Individual consent of risky behaviors may be appropriate."). The document addresses issues around remote control software, privacy, and other issues arising in the context of the Sony BMG DRM-protected CDs.

304. *Id.*

305. *Id.*

> Potentially unwanted software should ask for user consent before software technology is installed or uninstalled, or if any personal information about users will be collected during software technology installation or when the software application is running. After providing a prominent notice about what is about to occur, users should be presented with a clear, easy-to-understand choice. For the consent to be meaningful, the purposes for which the information is being collected and will be used should be stated in a matter reasonably understandable to the user. Nothing should happen unless users provide a clear, affirmative 'Yes' to whatever is proposed. If users choose not to agree, there should be no disruption or interference with the computing experience. There should not, as a condition to the supply of a product or

If we assume that courts will continue to treat EULAs and other notices as a proxy for a "meeting of the minds" sufficient to bind consumers to license terms, then HCI-Sec methods of improving feedback and control are useful tools to aid policy makers and the private sector in the creation of better notices and consent experiences. We believe the HCI-Sec principles should be a component of FTC action to develop security and privacy best practices and rules for software downloads based on the more stringent notice and consent procedures found in the Sony BMG and spyware decisions and orders.

The FTC is the natural place to build upon the work begun in the private sector, and to pull in additional expertise from disciplines including HCI-Sec, behavioral economics, and computer and information security to create best practices and potentially new rules to guide the interactions between consumers and businesses in the online environment. The FTC is far better suited to engage in the policy analysis and balancing required by this activity than the courts or even Congress. The need for flexible standards as opposed to hard and fast rules lends itself to the ongoing oversight of an agency, like the FTC, that can continue to revisit and alter standards as the market evolves.

Finally, improving the extent to which individuals understand that they are compromising security will not necessarily reduce the likelihood of such compromises if users acting in their own self interest nonetheless make poor security choices in a networked environment. Given the externalities posed by users' decisions to impair the security of their own machines—even those made knowingly, based on full and accurate information—the FTC must determine those terms to which users may not consent due to public policy concerns about the overall security of the information infrastructure.

VII. CONCLUSION

This Article set out to explain the market, technological, and legal factors that led Sony BMG toward a DRM strategy that, in retrospect, appears obviously and fundamentally misguided. Examining Sony BMG's long and unfortunate series of missteps offers important insights into necessary reforms of market practices, policy interventions, and the technology it-

---

> service, be a requirement for a user to consent to the collection, use, or disclosure of information beyond what is required to provide the services or applications in question without clear choices for the user."

Id.

self. The confluence of factors that encouraged, enabled, and failed to prevent Sony BMG's actions are complicated and interdependent. Unsurprisingly, we conclude that preventing similar future incidents requires approaches that incorporate technology and law and respond to the relevant market conditions.

Until average users are better equipped with intuitive tools and concise, compelling information describing relevant risks and benefits, they will be unable to manage the security of their machines. And unless users can take control of their security, we will be forced to choose between an increasingly insecure networked environment and one with diminished adherence to the end-to-end principle[306] as security management migrates from the desktop towards the center of the network.

Genuine end user control over security decisions relies on a level of transparency regarding the functionality and risks posed by software that can be assured only through independent public-minded security research. Such research can proceed at the necessary pace only once the threat of DMCA liability is lifted.

But the availability of information exposing these threats alone is insufficient. Both technology and law have a role to play in shaping usable security and privacy solutions. Technology can help to inform users and enforce their preferences to the extent those preferences can be accurately expressed and their violation detected. Users need the law to force the honest disclosure of terms and risks, and to protect them against overreaching license terms. And, in some rare circumstances, the law must prohibit certain risks that we cannot afford for users to accept in highly networked environments, regardless of their willingness.

If DRM is to emerge as a tool that benefits consumers through the introduction of new business models and innovative pricing structures, the terms of these transactions must be clearly and meaningfully presented to consumers. Unless consumers understand the rights granted and costs imposed by these transactions—among them sacrificed privacy and security—DRM will remain a tool that exclusively benefits copyright holders, while presenting consumers with, at best, inconvenience and, at worst, violations of their security, privacy, and expectations.

---

306. The end-to-end principle holds that complexity should be concentrated at the edges of a network rather than at its center. This principle gives rise to complex end points and relatively simple networks connecting them. *See generally* J.H. Saltzer, D.P. Reed & D.D. Clark, *End-to-end Arguments in System Design*, http://web.mit.edu/Saltzer/www/publications/endtoend/endtoend.pdf (1981).