TECHNICAL PROTECTION MEASURES FOR DIGITAL AUDIO AND VIDEO: LEARNING FROM THE FAILURE OF AUDIO COMPACT DISC PROTECTION

Mark H. Lyon†

Abstract

As consumers upgrade their computers, stereos and televisions they are replacing analog technologies with digital ones. These new technologies store information in a form that does not noticeably degrade as it is duplicated and is not bound to a particular recording medium. As the Internet bandwidth available to the average computer user has increased, has become highly efficient to transmit and share such data. Fearing enormous financial losses from widespread piracy, content providers sought methods to protect their content via technical protection measures ("TPMs").

Section I of this article provides a brief overview of technical protection measures. Sections II and III review various forms of technical protection measures that content providers have attempted to employ in connection with audio compact discs. Section III focuses specifically on Sony BMG's MediaMax and XCP measures and the resulting litigation. Section IV examines the new exceptions to the Digital Millennium Copyright Act's anti-circumvention rules. Section V explores the future of technical protection measures for sound recordings distributed on compact discs. Section VI looks at potential problems with technical protection measures in other digital media formats. Finally, Section VII suggests ideas on how content providers can avoid becoming the focus of the next copyright controversy.

† B.S. Mississippi College; candidate for J.D., Mississippi College School of Law, 2007. Lyon, Plaintiff in Lyon v. Sony BMG, launched the website SonySuit.com to share information with consumers related to litigation surrounding the 2005 Sony BMG Copy Protection Controversy. The author expresses his gratitude to those who provided their valuable insight and comments, including H. Lee Hetherington, Michael McCann, Gregory W. Bowman, and Kasey Nored.
I. INTRODUCTION

Consumers today are making enormous changes in the manner in which they consume music, movies, and other forms of entertainment. Increasingly, they are upgrading their computers, stereos, and televisions to improve the quality of their personal entertainment experience. Some are trading concerts and nights at the movie theater for the personalized entertainment environment that can now be created at home.¹ Unlike analog technologies, digital content does not noticeably degrade as it is duplicated.² Bits of data are not bound to the particular recording medium.³ Music stored on a compact disc can easily be stored on a hard drive in a computer, on the flash memory of the latest portable music player, and even backed up on digital tape for archival purposes.⁴

Internet bandwidth available to the average computer user has increased, making it highly efficient to transmit and share data through computer networks. One sale of a single compact disc in any record store could result in literally hundreds or thousands of near-perfect digital copies, all duplicated without the consent or control of the content producer or copyright holder. Fearing enormous financial losses from widespread piracy, companies that rely upon the sale of content sought methods by which they could protect their products.⁵

As the purchasers and users of digital content, regardless of the delivery method, become exposed to new technology which allows for the enjoyment of the latest movie or music, they will desire to

---


⁵ Recent studies indicate that the actual monetary loss from online, peer to peer digital copying of music appears to be somewhat less than initially feared. Felix Oberholzer-Gee of the Harvard Business School, in a study of 1.75 million downloads over a 17-week period in 2002, noted that the relationship between file sharing and subsequent sales is "statistically indistinguishable from zero." Beth Potier, *File Sharing May Boost CD Sales*, HARV. U. GAZETTE, Apr. 15, 2004, available at http://www.news.harvard.edu/gazette/2004/04.15/09-filesharing.html.
utilize their purchased content on a growing number of devices and in a striking number of new and imaginative ways. Technical protection measures which limit the usefulness of content, or which force users to purchase multiple copies of the same content, will in the future be increasingly faced with user discontent. This results in diminished market penetration and the promotion of alternative black markets of easily accessible pirated content.

Technical protection measures, if used in moderation, can be an effective method of limiting some forms of piracy. No technical protection measure will provide complete protection from unauthorized copying. Further, technical protection measures that abuse the trust of the consumer stand a great risk of being exempted from anticircumvention protection, opening up an entire class of digital content distribution methods to exploit. This latter problem is best demonstrated by the current state of technical protection measures for audio compact discs.

II. COMPACT DISC DIGITAL AUDIO

Phillips and Sony released the Compact Disc Digital Audio specification, known as the Red Book, in June of 1980. The specification, which must be licensed from Phillips, outlines the technical guidelines for the creation of interoperable audio compact discs. The Red Book standard has no provision for any form of technical protection measure.

While noncompliant, some content providers have attempted to utilize compact discs designed to be generally compatible with the Red Book, making them compatible with most standalone commercial compact disc players, but which have errors or special sections that make them unusable as audio discs on personal

6. The Sling Box, for example, is a hardware device that allows users to view and control their home entertainment systems through a residential Internet connection and a remote terminal such as a computer at work or a Windows Mobile PDA or Smartphone. See Sling Media, http://slingmedia.com/ (last visited Apr. 13, 2007).


8. Id.

computers and other devices capable of making copies of the digital audio content.  

Phillips, in an effort to protect interoperability with Red Book compliant devices of all types has restrained entities releasing noncompliant discs from the use of their trademarked “Compact Disc Digital Audio” logo.  

In some cases, the absence of this mark is the sole indicator that a product sold on the same shelves and at the same price as traditional audio compact discs is, in fact, something entirely different.  

Initial attempts at technical protection measures involved creating “hybrid” discs that contained multiple individual segments, known as “sessions.” One of these sessions would act as a traditional Red Book audio disc, while the remaining sessions contained computer data. When inserted into the CD-ROM drive of a typical computer, the device would ignore the audio portion of the disc and instead direct users to the information stored in the computer data session. Some methods took the additional step of selectively introducing errors into the audio session of the disc.  

One of the earliest methods of such error introduction is the Cactus Data Shield, released in late 1999. Audio, protected by the Cactus Data Shield, played normally in the majority of commercial standalone compact disc players, but when read by a device capable of detecting the malformation, such as a computer CD-ROM drive, would result in audio glitches. Malformation of the audio session

15. HALDERMAN, COPY-PREVENTION TECHNIQUES, supra note 13, § 4.1. See also Cactus Data Shield, supra note 14.
16. HALDERMAN, COPY-PREVENTION TECHNIQUES, supra note 13, §§ 4.2-4.3.
was largely discontinued due to incompatibility with some players and the improved error-correcting capabilities of modern CD-ROM drives, which could ignore errors introduced onto the disc.¹⁹

Later technical protection measures avoided intentional corruption of the audio data and instead focused on the inclusion of data tracks containing software that would be executed upon insertion into Windows or Macintosh computers.²⁰ Generally the software included on these discs would present an interface to the computer user, which allowed them to access "bonus content" or pre-encoded digital files that were protected against file sharing.²¹ Some included software would install programs on a user's computer to prevent access to the audio portion of the disc.²² Automatic execution of the included software could be disabled in both operating systems.²³

III. THE SONY BMG COPY PROTECTION CONTROVERSY

Sony BMG, one of the four largest music companies, began including certain technical protection measures, known as MediaMax and XCP in September 2003 and January 2005, respectively.²⁴ One of the two software programs was included on over one hundred different albums, with no identifiable pattern as to genre or artist.²⁵

¹⁹. HALDERMAN, COPY-PREVENTION TECHNIQUES, supra note 13, § 5.
²³. One computer science student who noted that the execution of such programs could be halted on Windows systems by simply holding down the left shift key while inserting a protected CD was threatened with a lawsuit alleging that such instructions, published as Princeton University Computer Science Technical Report TR-679-03, amounted to a circumvention method prohibited by the Digital Millennium Copyright Act. See Katie Dean, Shift-Key Case Rouses DMCA Foes, WIRED, Oct. 11, 2003, http://www.wired.com/news/digiwood/0,1412,60780,00.html.
The discs could be identified by their lack of the Phillips “Compact Disc Digital Audio” logo, an additional block of text on the back panel of the CD case which informed users that “[u]nauthorized copying is punishable under federal law,” and a short informational box indicating compatibility with various players or computer systems.\textsuperscript{26}

\textbf{A. Software}

Software was included and configured to begin running once it was inserted into the computer, utilizing a data session on the disc.\textsuperscript{27} With both MediaMax and XCP, the user would be confronted with a “clickwrap”\textsuperscript{28} end-user license agreement for the software and an option to install the program in order to access the audio files or digital content.\textsuperscript{29} The software was presented as a music player that would allow for protected digital copies of the songs on the disc to be played on the PC and “authorized” portable media players.\textsuperscript{30} It would additionally allow for a limited number of backup copies of the audio disc to be made.\textsuperscript{31} The software was described as being for the protection of the audio files on the disc.\textsuperscript{32} The license agreement indicated that the software could be removed, and that it would not collect personal information\textsuperscript{33}.

Once the XCP or MediaMax software was installed it began to continually operate on the user’s computer, even when no compact disc was inserted.\textsuperscript{34} The programs monitored all other similar music


\textsuperscript{29}Consolidated Amended Class Action Complaint, \textit{supra} note 24, ¶ 4.


\textsuperscript{31}\textit{Id.}


discs, and could not be easily uninstalled.\textsuperscript{35} The method for removing
the programs, which required a user to submit personal information to
Sony BMG through their website, did not actually remove either
application.\textsuperscript{36} Further, the software contacted Internet servers operated by
Sony BMG, leaving information in the company’s records
regarding the compact disc usage and listening habits of each user.\textsuperscript{37}

The XCP version of these Sony BMG discs created a number of
security vulnerabilities in a user’s Windows computer. These
vulnerabilities allowed not only the technical protection measure to
hide from users and prevent removal through the use of a “rootkit,”\textsuperscript{38}
but also allowed viruses or other malicious software to evade
detection by commercial anti-virus applications.\textsuperscript{39} A security patch,
released after controversy arose regarding the use of XCP,
unintentionally opened additional vulnerabilities, which allowed
remote hackers to install software or reboot a computer at will.\textsuperscript{40}
More than two million infected discs were created.\textsuperscript{41}

Some versions of the Sony BMG MediaMax discs installed their
software payload regardless of the user’s selection of the “agree” or
“disagree” option when presented with the “clickwrap” end-user
license agreement.\textsuperscript{42} The patches and uninstall routines provided by
Sony BMG again opened further vulnerabilities on a user’s
computer.\textsuperscript{43} The software was included on over twenty million discs
manufactured by or for Sony BMG.\textsuperscript{44}

\begin{footnotesize}
\begin{enumerate}
\item Consolidated Amended Class Action Complaint, supra note 24, \makebox[0.5in]{\textsuperscript{23-32.}}
\item Id. \makebox[0.5in]{\textsuperscript{\textsuperscript{26}.}}
\item Id.
\item Bruce Schneier, \textit{Real Story of the Rogue Rootkit}, \textit{WIRED}, Nov. 17, 2005, http://wired-
vig.wired.com/news/privacy/0,1848,69601,00.html. A rootkit is a set of tools designed to
conceal running programs or files from the operating system. \textit{See generally} Bryce Cogswell &
Mark Russinovich, Microsoft TechNet, RootkitRevealer v1.71 (Nov. 1, 2006),
\textit{See also} Groklaw, EFF’s Sony Complaint Includes MediaMax & Unconscionable EULA
Claims, http://www.groklaw.net/articlebasic.php?story=20051121215116613 (Nov. 21, 2005,
22:23 EST) \textit{[hereinafter Groklaw, Sony Complaint].}
\item Groklaw, Sony Complaint, supra note 38.
\item Schneier, supra note 38; Groklaw, Sony Complaint, supra note 38.
\item Groklaw, Sony Complaint, supra note 38.
\item Halderman, MediaMax, supra note 22.
\item Consolidated Amended Class Action Complaint, supra note 24, \makebox[0.5in]{\textsuperscript{23-32.}} \textit{See also}
Groklaw, Sony Complaint, supra note 38.
\item Groklaw, Sony Complaint, supra note 38.
\end{enumerate}
\end{footnotesize}
B. Sony BMG's Response

Sony BMG had been alerted to the risks of their software on September 30, 2005 and October 4, 2005 by anti-virus vendor F-Secure, but those risks were not made public at that time. The risks associated with XCP were first released publicly by Mark Russinovich on October 31, 2005. In his blog post, Russinovich offered a highly technical description and examination of the Sony BMG XCP rootkit. Word quickly spread throughout the online community.

Initially, Sony BMG was slow to respond to the concerns of users. On November 4, 2005, during an interview with National Public Radio's Morning Edition, Thomas Hesse, President of Sony BMG's global digital business division asked: "Most people don't even know what a rootkit is, so why should they care about it?"

Initially, users who requested the uninstaller tool from Sony BMG's website were not provided with the tool they requested. Calling Sony BMG at the phone numbers listed on their website resulted in little assistance to users concerned about their safety and security of their computers. Nearly a month later, information on removing the software was not available from Sony BMG, and the

46. Mark Russinovich is a Technical Fellow in the Platform and Services Division at Microsoft. He was the co-founder and Chief Software Architect of Winternals Software, and has written numerous administration and diagnostic utilities for the Microsoft Windows operating system. For more information or to contact Mr. Russinovich, visit http://blogs.technet.com/markrussinovich/about.aspx.
47. Mark's Blog, Sony, supra note 34.
48. See id.
company had not taken effective steps to remove the discs from the marketplace.\textsuperscript{53}

Dr. Larry Ponemon, in an affidavit for the Electronic Frontier Foundation, estimated that 1.44 million computers were infected with XCP or MediaMax, and determined the time lost by the class members to have a value of up to $32.76 million dollars.\textsuperscript{54}

\textbf{C. Anti-Virus Vendor Response}

It is important to note that a number of major anti-virus vendors were aware of the Sony BMG XCP and MediaMax software, but took no affirmative steps to correct its behavior.\textsuperscript{55} No antivirus program protected consumer’s computers from malicious software hiding under the protective cloak provided to it by the Sony BMG software. Methods of removing the infection were delayed until long after the dangers of the software were well known.\textsuperscript{56}

The anti-circumvention provision of the Digital Millennium Copyright Act\textsuperscript{57} ("DMCA") was cited by researchers and anti-virus vendors as the primary reason for not alerting users or providing methods for removing or disabling the Sony BMG software before the public became aware of the risks posed by Sony BMG’s software.\textsuperscript{58}

As a result, Sony BMG’s XCP and MediaMax were allowed to silently spread to at least 568,200 public, private, educational, and military networks worldwide.\textsuperscript{59}

As previously noted, antivirus vendor F-Secure alerted Sony BMG to the risks of their software on September 30, 2005 and October 4, 2005.\textsuperscript{60} They did not, however, immediately offer a


\textsuperscript{54} Declaration of Larry Ponemon in Support of the Ricciuti Class Representatives’ Memorandum of Law in Support of Motion for an Award of Attorneys’ Fees and Reimbursement of Expenses, In re Sony BMG CD Technologies Litigation, No. 1:05-cv-09575-NRB (S.D.N.Y. Apr. 6, 2006).

\textsuperscript{55} Schneier, supra note 38.

\textsuperscript{56} Dan Kaminsky, Learning from Sony: An External Perspective, VIRUS BULL., Feb. 2006, at 8.


\textsuperscript{60} Hamm, supra note 45.
method for removing XCP or MediaMax to their customers. Instead, they attempted to work with Sony BMG to correct the security risk. Those talks were still ongoing when Mark Russinovich released his report.

McAfee added detection code to their anti-virus utility on November 9, 2005. Instructions and methods for removing the XCP software were made available by Sony BMG on December 6, 2005. The McAfee anti-virus application contains an option to allow the Sony BMG software to remain on a computer, warning users that they may have a legal obligation to do so.

Symantec released a utility on November 10, 2005 that removed the "cloaking" feature from the Sony BMG software. Their utility does not remove the program; it instead instructs users to update infected computers with the latest version of the Sony BMG software in lieu of removal with the following message:

WARNING: Removing this security risk manually may damage the compromised computer's operating system and may violate the manufacturer's end-user license agreement.

Symantec Security Response strongly recommends installing the software update provided by the manufacturer. The latest version removes the security risk from the compromised computer and replaces it with an updated version of the XCP software. This update is available at the following URL:

http://cp.sonybmg.com/xcp/english/updates.html

Microsoft, whose Windows operating system could at times be unstable when infected with the Sony BMG software, did not

---

61. Id.
62. Id.
63. Id.
64. Schneier, supra note 38.
68. Id.
announce until November 13, 2005 that it would provide a tool to remove the infection.69

D. Class Action Litigation

Dissatisfied with the response from Sony BMG, a number of individual and class action lawsuits were filed throughout the United States and other countries.70 The majority of the US cases were consolidated in the United States District Court for the Southern District of New York.71

Amongst the many class action claims were violations of the Computer Fraud and Abuse Act, which prohibits accessing a computer without, or in excess of, the authority granted by the owner of the computer; common law trespass to chattels, and unfair or deceptive business practices.72 In some states, most notably California73 and Texas74, claims included state causes of action designed to prohibit "spyware" or other malicious software.75

Once the matters were consolidated, Sony BMG’s attorneys worked quickly to reach a settlement. On December 28, 2005, Sony BMG’s attorneys and class counsel Scott Kamber submitted to the court a motion requesting approval of a proposed settlement.76

The settlement provided for a replacement of infected discs. Additionally, it offered the option of either $7.50 in cash and one album download, or three album downloads with no cash incentive.77 Consumers were allowed to select from a catalog of two hundred albums from Sony BMG artists at several different music download

71. Consolidated Amended Class Action Complaint, supra note 24.
73. CAL. BUS. & PROF. CODE § 22947.3 (West 2007).
sites, including Apple's iTunes service. The settlement was approved by District Judge Naomi Reice Buchwald in 2006.

A number of State Attorneys General also filed consumer protection or other related actions against Sony BMG. California and Texas, along with thirty-nine other states, settled their claims with Sony BMG for approximately $4.25 million in fines and legal fees in different actions in December of 2006. The settlements also provided additional benefits to consumers, including up to a $175 payment to individuals who could demonstrate expenses for removing the software from their computer, or a $25 payment to those who did not retain such documentation, or who were able to remove the infection themselves.

IV. DMCA ANTI-CIRCUMVENTION EXCEPTIONS

The greatest fallout from the Sony BMG Copy Protection Controversy was not the cost to the company or their damaged reputation in the marketplace. The strongest impact would be felt one year later, on November 27, 2006, when the Librarian of Congress announced new classes of works exempt from the prohibition against circumvention of technological protection measures controlling access to copyrighted works under the Digital Millennium Copyright Act (DMCA).

The DMCA contains provisions that make the circumvention of technical protection measures, no matter how poorly planned or
implemented, punishable through civil and criminal action. The civil penalties applicable to § 1201 circumvention, an act which many contend removing XCP or MediaMax to be, include a fine of not less than $200 nor more than $2,500 for each act or offer of circumvention. Additionally, those who undertake § 1201 circumvention for “commercial advantage or private financial gain” risk $500,000 fines and a maximum of 5 years imprisonment for the first offense; double penalties apply for each subsequent circumvention. With the possibility of such serious repercussions, it is understandable that antivirus vendors took a cautious stance when approaching the removal or disabling of Sony BMG’s technical protection measures.

The new exceptions remain in effect until October 27, 2009. One directly addressed the Sony BMG Copy Protection Controversy. It allowed the circumvention of technical protection measures associated with:

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

Opponents of the exception correctly noted that allowances were already made in the DMCA “for the purpose of good faith testing, investigating, or correcting, a security flaw or vulnerability, with the authorization of the owner or operator of such computer, computer system, or computer network.” In response, Marybeth Peters, the United States Register of Copyrights, while making her office’s recommendation to the Librarian of Congress, noted that “while it appears that this statutory exemption may permit circumvention in cases such as those involving MediaMax and XCP, it is not clear

---

88. Exemption to Prohibition on Circumvention of Copyright Protection Systems for Access Control Technologies, supra note 84.
89. Id. at 68,477.
whether that provision extends to such conduct." The Register of Copyrights then recommended the exception for those legitimate efforts to investigate or correct the security risks noted in § 1201(j).

While narrowly drawn, this exception effectively permits the circumvention of almost every known form of technical protection measure for audio compact discs. For a technical protection measure to be effective, it must exert a level of control over the computer system. Sony BMG's XCP software inserted pieces of software code between the different portions of the operating system responsible for accessing the CD-ROM drive. When protected content was detected, the injected code would provide false information to the operating system.

Such operation relied upon an insecurity of the Microsoft Windows device driver model, which allowed programs to install software that would interfere with the correct operation of the CD-ROM drive. Similar methods for providing independent security of digital content will, by necessity, involve further exploitation of vulnerabilities within the operating system in order to cause the system to operate differently than intended. Almost any exploitation of weaknesses in an operating system can lead to compromised computer security. With the implementation of the above DMCA exception, the viability of even marginally effective current technological protection measures for audio recordings distributed via the compact disc was totally eliminated.

V. THE FUTURE OF TECHNICAL PROTECTION MEASURES FOR SOUND RECORDINGS DISTRIBUTED IN COMPACT DISC FORMAT

The Sony BMG Copy Protection Controversy and the resultant DMCA exception signaled the end of the current phase of technical

91. Exemption to Prohibition on Circumvention of Copyright Protection Systems for Access Control Technologies, supra note 84, at 68,477.
92. Id.
protection measures included on audio discs. Consumer fear and distrust of the music and antivirus industries helped to push consumers away from protected discs. NVPI, the Dutch entity responsible for the promotion and support of the music industry, announced in January of 2007 that EMI, a major music label, was the final label to remove technical protection measures from new audio discs sold in their country.  

No such official announcement has been released by the Recording Industry Association of America, but anecdotal reviews of record store shelves indicate that a number of newer discs still contain some limited forms of technical protection measures. Increasingly, the current form of technical protection measure involves the insertion of a data session containing "bonus content" and/or protected digital copies of the music on the disc, but no software designed to prevent users from accessing or copying the Red Book compliant portion of the audio disc. The Recording Industry Association of America has enacted a standards document that requires such discs to be playable in any complaint compact disc player.

The 2007 EMI Records release, Lily Allen – Alright, Still, contains one such data session of bonus content. Upon insertion of the disc into a Windows computer, the disc launches an application called “U-MYX” which allows users to create their own remix of two songs from the album. Users are allowed to selectively control the vocals, background sounds, instrumentation, percussion, and other

99. Generally, these compact discs are referred to in the marketplace as an “Enhanced CD” and are available from a number of different record labels.
101. This modern musical release is available at http://www.amazon.com/Alright-Still-Lily-Allen/dp/B000FMSGWRS.
aspects of the songs. Users are able to access and play the audio portion of the disc independent of the included software.

Such "added value" content is growing in popularity as a replacement for more draconian technical protection measures. Additional content provides a mechanism by which users can become more familiar with the artist or explore more of the content they enjoy. Further, the additional data session somewhat complicates the process of duplicating the disc for the casual user while at the same time offering an additional benefit to users who purchase the disc. Because the included software does not attempt to monitor or control the consumer's computer, users can be assured that the risk of exploitation or the creation of security vulnerabilities is minimal.

At the current time, the market does not appear to be prepared to accept strict technical protection measures on audio discs. Continued and increased inclusion of bonus content may serve to help overcome the negative effects of the Sony BMG XCP and MediaMax software, and may lead the way for more effective and secure technical protection measures that may later be developed.

VI. POTENTIAL FOR SIMILAR PROBLEMS WITH OTHER TECHNICAL PROTECTION MEASURES IN OTHER FORMS OF DIGITAL MEDIA

The widespread distribution of news regarding Sony BMG's rootkit helped inform consumers of the harm that could result from poorly designed or implemented technical protection measures, and sparked considerable debate about technical protection measures in other forms of content, such as downloadable music and next-generation high definition video discs.

Consumer discontent over the risks revealed by the Sony BMG Copy Protection Controversy may help to drive future concerns about technical protection measures that remove control of a consumer's equipment from their hands. With the growing adoption of high definition televisions, digital broadcast radio, and other new technologies, content providers are at a new crossroads where hard choices regarding technological protection measures must be made.

104. Examples of remixed versions of songs from the disc are available at http://www.u-myx.com/Music/Lily-Allen/Smile/.

105. For further information about the U-MYX software, and a demonstration video, visit http://www.u-myx.com/About/.

A. Digital Video Disc and High Definition Television

The now-familiar Digital Video Disc (DVD) is changing to meet the increased demands of consumers for high definition content. Traditional DVDs, introduced in the 1990s,\(^\text{107}\) can hold a large amount of video and audio information, but lack the capacity needed to provide high definition content.\(^\text{108}\) Their primary technical protection measures, the Content Scrambling System and Region Coding, have proven ineffective when faced with inventive programmers who have created software capable of decoding the protected content without properly licensed software or access keys.\(^\text{109}\)

New disc formats, such as the HD DVD and the Blu-ray Disc, offer much greater data capacities, allowing for high-definition video to be stored in the same form factor as a traditional DVD.\(^\text{110}\) These disc formats have been designed with new technical protection measures, including systems to ensure that unencrypted digital output cannot be captured through the use of untrusted hardware or software.\(^\text{111}\) These systems rely on a secure signal transport system from the disc player to the output device such as a television or computer monitor.\(^\text{112}\) With these systems, content providers can choose to degrade the quality of the signal if the transmission path cannot be verified as secure.\(^\text{113}\) Errors in the verification process have caused some consumers to experience degraded performance who

---

have done nothing to disturb the security of the transmission path.\textsuperscript{114} At least one security researcher has alleged that these technical protection measures may have serious fundamental flaws that undermine their effectiveness, but has not published his results due to fears of legal action.\textsuperscript{115}

Newer versions of some operating systems, such as Microsoft’s Vista operating system, include such technical protection measures for high definition content.\textsuperscript{116} This protection does not rely on outside software, but instead utilizes software and hardware pre-installed on a user’s computer by the operating system manufacturer.\textsuperscript{117} To facilitate this security, many computer systems of even recent vintage are not capable of displaying high definition content, as their hardware is not trusted by the operating system to enforce copy protection.\textsuperscript{118} The software and hardware involved in performing these tasks limits the control that users can exert over their computer systems, and has been rejected as draconian by some consumers.\textsuperscript{119}

If the scope of the audio disc anti-circumvention exception were expanded to include all technological protection measures that create or exploit security flaws or vulnerabilities that compromise the security of personal computers, it may be quickly found that the additional code necessary to implement even such embedded protection measures could cause such methods to be subject to circumvention. Further, even with these new protection methods, the ability of individuals wishing to defeat such systems has not been abated. As of January 2007, the technical protection measures of both the HD DVD and the Blu-ray Disc have been defeated.\textsuperscript{120}

---


\textsuperscript{117} Id.


B. Digital Downloads

Digital download services are divided into two different categories, those that offer a per-item purchase model and those that offer a subscription-based model. In the per-item model, users pay for each and every download, which they then expect to operate in perpetuity. With the subscription model downloads may be unlimited or limited to a certain number of downloads per time period, and users are allowed use of the downloaded content for as long as they continue to pay for their subscription.

Technical protection measures have created the market for the subscription-based model. Such measures, including those developed by Microsoft, Real Networks, and Apple, allow for the verification of the right to access content over the Internet, and for the revocation of access at will. While these systems are vulnerable to exploit, the effort involved in removing the protection measures from the downloaded files is often outweighed by the minimal recurring cost to maintain the subscription.

Per-item downloads are often protected with a technical protection measure that ties their playback to those devices and computers owned by an individual. Many consumers who are hesitant to purchase protected digital downloads are attracted to the prospect of the convenience and flexibility that is offered by unprotected digital downloads.

On February 6, 2007, Steve Jobs, CEO of Apple, published an open letter indicating a desire for record companies to allow his popular iTunes music service to remove its technical protection measures and offer unprotected music downloads. Jobs, writing

---

about digital rights management ("DRM"), the technical protection measure utilized by iTunes, said:

In 2006, under 2 billion DRM-protected songs were sold worldwide by online stores, while over 20 billion songs were sold completely DRM-free and unprotected on CDs by the music companies themselves. The music companies sell the vast majority of their music DRM-free, and show no signs of changing this behavior, since the overwhelming majority of their revenues depend on selling CDs which must play in CD players that support no DRM system.

So if the music companies are selling over 90 percent of their music DRM-free, what benefits do they get from selling the remaining small percentage of their music encumbered with a DRM system? There appear to be none. If anything, the technical expertise and overhead required to create, operate and update a DRM system has limited the number of participants selling DRM protected music. If such requirements were removed, the music industry might experience an influx of new companies willing to invest in innovative new stores and players. The music companies can only see this as a positive.128

Drawbacks of technical protection measures in downloaded content are primarily device lock-in and the related problem of portability.129 Individual tracks on the iTunes music service cost $0.99.130 Assuming that a user purchased just three tracks per month, spending $2.97 per month, she could quickly amass a collection of music valued at $71.28 in just two years. Such an amount rivals the cost of many music players, including Apple's own iPod shuffle.131 Consumers who choose to purchase a competing music player may find themselves unable to listen to their content on the new devices. Consumers who choose to remain with the iTunes platform will also soon find that their purchases are limited to activation on but five

---

128. Id.
devices, limiting their ability to listen to their purchased content in multiple locations.\textsuperscript{132}

Steve Jobs accurately understands the need to loosen restrictions on digital downloads. Continually burdening legitimate consumers with usage restrictions on purchased content will not attract the majority of consumers, especially when unprotected content is available at a comparable or lesser price. Digital content delivery gains its greatest benefit from convenience and immediacy. Users who find that they are not allowed to enjoy their purchased content in the manner or method they so choose will simply select another method of purchase, such as unprotected audio CDs, or will seek to obtain the content in violation of the content producer’s rights, through peer-to-peer or other black market channels, if the latter options present less difficulty for the content-seeking consumer.

VII. AVOID BECOMING THE FOCUS OF THE NEXT COPY PROTECTION CONTROVERSY

The Sony BMG Copy Protection Controversy resulted in a serious change in the landscape for technical protection measures. Moving forward, it is important that entities understand and examine the technical, legal, and business mistakes that were made, to ensure that if their organization is placed in a similar situation they react more effectively and favorably to the demands of their consumers. Content providers should keep several considerations in mind when selling protected content to guard against the risks of technical protection measures that could adversely impact the sales of content.

First and foremost, the presence of a technical protection measure and any restrictions imposed should be fully and accurately explained to the customer, both before purchase and before installation. In some business models, such as the subscription digital download, the presence of a software component is a necessary requirement for the function of the service. Some content, because of the inclusion of a technical protection measure, may be offered at a lower cost than unprotected versions of the same content. In such cases, it is important that consumers understand which rights, including the various “fair use” rights, which will or will not be granted to the content. Consumers should be able to easily access resources that will explain what they should expect, and if the

protective measure is installed on their computer or other equipment, the installation should not be hidden from the consumer's view. Consumers who desire to return digital content during a short period of time following their purchase due to problems, errors, or technical difficulties should be offered refunds. Exchanges of digital content returned for these reasons is an inadequate solution, as replacement content will likely not be available with alternative technical restrictions.

Furthermore, the customer should explicitly authorize any communication by the technical protection measure to a remote system before that communication occurs. Preferably, the authorization should happen at the time of the communication. Information gathered by the technical protection measure should not be retained for a longer period than necessary for the operation of the protection measure, and should not be used to compromise the confidentiality of the customer. As our lives are increasingly computerized, many consumers fear the loss of control over their personal information. Even information as simple as the preference for rap over country music could be a detail that a consumer would desire to keep private. Unnecessary communication should be avoided, and communication with remote systems should be governed by a clear privacy policy, with the reason for the communication clearly explained to the consumer.

When possible, interoperable technical protection measures should be utilized. By allowing users the freedom and flexibility to use their purchased or rented content, across multiple devices from a wide range of manufacturers, would reduce the "lock in" experienced by users of many current systems, and could help overcome some objections by those unwilling to purchase protected content.

Any installed technical protection measure must be capable of being fully and completely removed at will by the customer. The lack of a clear and accessible removal method was the primary pitfall of Sony BMG's XCP and MediaMax. The temptation to disable removal functionality is certainly great, as an uninstalled technical protection measure is no protection at all, but it is important to consider that the software is installed on a device owned by the consumer, not the content provider. Offering clear warnings that protected content will not be accessible after removal is certainly an acceptable step, but should be the only impediment to the consumer's decision to uninstall any added software.

Additionally, Sony BMG's XCP and MediaMax demonstrated that technical protection measures could inadvertently create security
flaws or vulnerabilities that could compromise the security of personal computers. All software included with content should be tested, verified, and publicly certified by at least one independent testing agency. Such independent analysis and certification would add a trivial cost to most major technical protection measures, but would offer a level of comfort and protection for both the consumer and the content provider.

Finally, content providers should carefully examine the actual risks and benefits to be experienced by offering some or all of their content without technical protection measures. History has demonstrated that technical protection measures will be compromised nearly as fast as they can be created, and that they rarely impact commercial piracy. Watermarking and other source verification methods may provide an effective tool for the tracking of digitally obtained content. This method can help prevent unauthorized file sharing, since the source of a shared file can be identified, while at the same time allowing consumers to personally use their purchased content in any lawful manner they choose. The time, effort, and resources that must be devoted to the creation of protection measures may be better dedicated to bringing new and exciting content to the marketplace.

Missteps will be made in the development and implementation of future technical protection measures. Most of these failures will be minor, and easily corrected. Some, however, may not be so benign. It is important that entities implementing technical protection measures learn from the failures of Sony BMG. Organizations can limit their potential for becoming the focus of the next copy protection controversy by providing advance notice to consumers of the potential risk, carefully crafting a design and implementation strategy that respects the consumer and their equipment, and by working quickly to communicate and correct any vulnerabilities as they are discovered.