DRM OR SPYWARE: DID SONY GO TOO FAR?

Adam Marcus

Introduction

On October 31, 2005, a DRM monster was revealed. DRM stands for Digital Rights Management, and is one of the names for technology that copyrightholders use to protect their works from being accessed or used in ways and by individuals they don't approve of. DRM is preferred over simply relying on copyright laws because DRM protections don't require the copyrightholder to sue infringers. Whereas copyright laws provide *ex post* analysis of whether a user's actions violate copyright laws, DRM allows copyrightholders to decide *ex ante* which actions they will allow and prevents all others.

On that fateful Halloween eve, Mark Russinovich posted to his Sysinternals Blog about a piece of software included with the Van Zant CD "Get Right With the Man," released by Sony BMG. The software, which installed itself on his computer without his permission, notifies Sony every time a song from the CD is played, and makes the computer more vulnerable to viruses, trojan horses, and spyware (because they can piggyback on the same cloaking technique to avoid detection by antivirus/antispyware software).[1] Russinovich's blog post sparked a controversy that resulted in the Texas Attorney General filing a class action lawsuit, two other State Attorneys General initiating investigations, a national class action suit, three class action suits in Canada, and a preliminary criminal investigation in Italy.[2] The legal actions are centered on

[1] http://www.sysinternals.com/blog/2005/11/more-on-sony-dangerous-decloaking.html

[2] See http://www.sonysuit.com

whether the Sony DRM should be considered "spyware." Not surprisingly, all of the lawsuits filed against Sony have been or are in the process of being settled. But the legal questions raised in these lawsuits will likely be seen again in the future.

This paper will explain how the Sony software works, what laws Sony and the designer of its DRM software may have violated, and what copyrightholders can do in the future to protect their works without running afoul of the law. Rather than analyze the laws of each state, this paper focuses on California's Consumer Protection Against Computer Spyware Act. As one of the first states to enact anti-spyware legislation, California's law served as a model for many other states.[3] Although there are federal computer crime laws, none are specifically tailored to deal with spyware.

Sony's DRM Software

Before delving into the details of Sony's DRM software, the reader must understand a few basics about CDs and MP3s. A standard audio CD contains a number of audio tracks. Each track is essentially an uncompressed audio file. A three minute song takes up approximately thirty megabytes of storage space on the CD. The MP3 format is a compressed audio format. The same three minute song takes up only three megabytes as a MP3 file. CD "ripping" software extracts the uncompressed audio tracks from a CD and converts the tracks to MP3 files. Sony's goal in using DRM software was attempting to prevent users from extracting the audio tracks from the CDs, converting them to MP3 format, and illegally sharing those tracks with others, usually via peer-to-peer networks.

[3] See http://www.ncsl.org/programs/lis/privacy/eprivacylaws.htm

The CD audio standard was finalized before the DMCA, and thus has no copy protection of any type. Because of this, it is completely legal to manufacture and distribute ripping software, and the holding of the Universal City Studios v. Sony case, which allowed time-shifting broad television shows, has been interpreted to also allow space-shifting (AKA format-shifting) of CD audio to portable MP3 players. XCP and MediaMax are examples of copyrightholders attempting to prevent ripping CD tracks to MP3 format yet still allowing those CDs to play in stand-alone CD players.

Sony's DRM-protected CDs contain two "sessions": a standard audio session that is no different than a DRM-free CD, and a data session that can be read by computers. Stand-alone CD players ignore the data session and just play the tracks in the audio session. When a multi-session CD is inserted into a computer, the computer looks at the data session first. Microsoft Windows has a feature called AutoRun that allows software developers to have a program on a CD run automatically when a CD with a data session is inserted into a computer. It is this AutoRun feature that Sony's DRM software uses to get installed on users' computers.

There are two different software programs that Sony has used to protect its CDs: First 4 Internet's Extended Copy Protection (XCP) and Suncomm's MediaMax. It was XCP that was first identified by Russinovich on October 31, 2005. On November 12, 2005, J. Alex Halderman identified Suncomm's MediaMax software, which was included on other Sony music CDs, as having serious security issues of its own.[4]

The first time an XCP-protected CD is inserted into a Windows computer, an End User License Agreement (EULA) appears that the user must agree to before the software is installed.

[4] http://www.freedom-to-tinker.com/?p=925

The EULA states that “SONY BMG and each LICENSOR reserve the right to use the SOFTWARE and/or any APPROVED MEDIA PLAYER to enforce their respective rights in and to the DIGITAL CONTENT … at any time, without notice to you.” But the EULA also states that “Once installed, the SOFTWARE will reside on YOUR COMPUTER until removed or deleted. However, the SOFTWARE will not be used at any time to collect any personal information from you, whether stored on YOUR COMPUTER or otherwise.”

The SOFTWARE referred to in the EULA consists of a player application to play the songs on a computer and the “rootkit.” The rootkit is designed to prevent ripping software from extracting the audio tracks (referred to as “audio files” in the Sony EULA) from the CD. It does this by installing software that replaces the normal device driver for the CD-ROM drive. The XCP driver prevents all applications other than the XCP player from accessing XCP-protected CDs. When the player application is used to play a song from the CD, it also “phones home” to a Sony server. This system was designed to allow Sony to update the banner that displays at the bottom of the player window, but can also be used to track when users play songs. Because this system uses the standard HTTP protocol, the requests include the IP address of the user’s computer, the operating system installed on the computer, and the version of Internet Explorer installed on the computer. This information is arguably “personal information”, but presumably Sony is bound by its own EULA to not use these requests to track users.

Besides the fact that XCP is installed without adequate disclosure of what is does, it could cause serious problems for users. The fact that the EULA mentions the software being removed or deleted could be taken to imply that the software can be removed using the standard Windows ‘Add/Remove Programs’ function. That is not the case. XCP uses non-standard programming techniques to completely hide its existence from users and there is no obvious way

to uninstall it. The technique used to hide XCP, once XCP is installed, can be used by other software to intentionally damage a user's computer and avoid detection by anti-virus software. At least one virus has been designed specifically to take advantage of this.[5] XCP also permanently degrades the computer's performance by two percent, even when the Sony music CD is not being played.[6] Even worse, XCP itself can cause the computer to crash.[7] Finally, attempting to manually uninstall XCP could cause a user's CD-ROM drive to stop working.

MediaMax is similar to XCP with two exceptions, one good and one bad. The good thing about MediaMax is that it does not have the "cloaking" functionality that XCP has, so its files are visible to users and virus software can't piggyback on the cloaking functionality to infect computers. The bad thing about MediaMax is that it has what was likely a software bug that can result in the software being installed even if a user does not accept the EULA.[8]

California's Consumer Protection Against Computer Spyware Act

The key to distinguishing spyware from other types of software is notice to and consent from the end-user about what the software is doing. The Anti-Spyware Coalition, comprised of anti-spyware software companies, academics, and consumer groups, is dedicated to building a consensus about definitions and best practices in the debate surrounding spyware. It defines spyware as follows:

> Technologies deployed without appropriate user consent and/or implemented in ways that impair user control over: (1) Material changes that affect their user

[5] http://www.eff.org/deeplinks/archives/004150.php

[6] http://www.sysinternals.com/blog/2005/10/sony-rootkits-and-digital-rights.html

[7] http://www.sysinternals.com/blog/2005/11/sonys-rootkit-first-4-internet.html

[8] http://www.freedom-to-tinker.com/?p=936

> experience, privacy, or system security; (2) Use of their system resources, including what programs are installed on their computers; and/or (3) Collection, use, and distribution of their personal or other sensitive information.[9]

California's spyware law is similar. Although it doesn't define spyware, it does list a number of acts that are prohibited unless adequate notice is provided.[10] The most relevant section of the statute for purposes of the Sony DRM software is Section 22947.3(c), which prohibits a person or entity that is not an authorized user from causing computer software to be copied onto the computer of a consumer in California and using that software to prevent an authorized user's reasonable efforts to block the installation of, or to disable, software, by presenting the user with an option to decline installation of software with knowledge that, when the option is selected by the authorized user, the installation nevertheless proceeds. MediaMax clearly violates this provision, as the software is installed before the End-User License Agreement (EULA) is displayed and is not uninstalled if the EULA is declined. But the mens rea for this act is "actual knowledge, with conscious avoidance of actual knowledge, or willfully." To avoid liability, Suncomm and Sony would have to convince a court that their testing procedures were not so lacking that they constitute "conscious avoidance of actual knowledge." Even though the installation mistake is a bad one, it probably doesn't rise to the level of conscious avoidance.

Section § 22947.3 also contains an exemption stating that it does not apply to "any monitoring of, or interaction with, a … protected computer, by a … computer … software provider … for … computer security purposes … or detection or prevention of the unauthorized use of or fraudulent or other illegal activities …" The Assembly Committee on Business and

---

[9] http://www.antispywarecoalition.org/documents/DefinitionsJune292006.htm

[10] Consumer Protection Against Computer Spyware Act, codified at Cal. Bus. & Prof. § 22947.

Professions analysis of the amendment which added this exemption stated that it was "taken from federal law," but that isn't quite accurate.[11] The exemption in the California bill seems to have come from the Securely Protect Yourself Against Cyber Trespass Act (SPY ACT), introduced by Representative Bono on July 25, 2003.[12] California's spyware statute is similar to language that first appeared in the federal bill as passed by the House of Representatives on October 5, 2004.[13] The federal bill limits monitoring for the purpose of determining whether the user of the computer is authorized to use such software only upon "initialization of the software; or an affirmative request by the owner or authorized user for an update of, addition to, or technical service for, the software."[14] The California bill is much broader. It exempts any monitoring for the "detection or prevention of the unauthorized use of or fraudulent or other illegal activities in connection with a network, service, or computer software."[15] Some have suggested this expansive language was introduced at the behest of the Motion Picture Association of America and the Recording Industry Association of America.[16] Although it seems unreasonable for a law meant to combat spyware to explicitly allow the unauthorized installation of monitoring software on consumers computers (for that is precisely the definition of spyware),

---

[11] Analysis prepared by Hank Dempsey for August 10, 2004 hearing of the Business and Professions Committee. Available at http://info.sen.ca.gov/pub/03-04/bill/sen/sb_1401-1450/sb_1436_cfa_20040809_100201_asm_comm.html

[12] H.R. 2929.

[13] H.R.2929.EH, at http://thomas.loc.gov/cgi-bin/query/D?c108:3:./temp/~c108Omdkov::

[14] H.R.2929.EH Sec. 5(b)(2).

[15] Cal. Bus. & Prof. Code § 22947.3(d).

[16] See Dimo Michailov, "California's Anti-Spyware Crusade," January 2, 2004, at http://www.cybercrimelaw.org/blog/28/California%27s+Anti-Spyware+Crusade.html

that seems to be exactly what this exemption does—as long as the purpose is detection or prevention of unauthorized use.

The exemption in § 22947.3 doesn't apply to § 22947.4, which prohibits unauthorized user from inducing an authorized user "to install a software component onto the computer by intentionally misrepresenting that installing software is necessary for security or privacy reasons or in order to open, view, or play a particular type of content."[17] The XCP EULA arguably violates this statute because it states "if you do not agree to be bound by these terms and conditions, you will not be able to utilize the audio files or the DIGITAL CONTENT on YOUR COMPUTER." Because XCP-protected CDs contain a standard audio session, they can be played by a computer with no additional software. Curiously, the quoted statement seems to directly contradict the first sentence in the EULA: "This compact disc ('CD') product contains standard so-called 'Red Book'-compliant audio files that can be played on any standard CD player, including those contained in many personal home computer systems." Although CDs with XCP and MediaMax can contain additional songs, artwork, videos, and other interactive content, the current XCP and MediaMax EULAs don't clearly explain that the software is only required for the additional content and not for the audio tracks. But it is the audio tracks and not the additional content that these DRM schemes are designed to protect.

Liability

Because California's spyware law was designed to combat spyware and not overreaching copyrightholders, if copyrightholders give adequate notice about the purpose and operation of their software, they are not likely to be liable for violating California's spyware laws. One of the

[17] Cal. Bus. & Prof. Code § 22947.4(a)(1).

lawsuits filed in California based additional claims on the Consumer Legal Remedies Act ("CLRA"), which prohibits, among other things, representing to consumers that a good has characteristics and benefits that it doesn't have.[18] But even these claims can be avoided with adequate notice. This is generally true for spyware as well as DRM software.

Alternatives

Even if MediaMax and XCP did not violate any laws, Sony's efforts at preventing the sharing of unprotected copies of its songs were futile. These programs have no effect on other operating systems, users of CDs with XCP can refuse the EULA and not install the software, and users can always still access the tracks using the "analog hole."[19] Furthermore, once a single user has obtained an unprotected digital copy of a work, they can make an infinite number of copies with no loss in quality. Thus, once a single user has shared a work on a peer-to-peer network, it's quite possible that the work will be propagated to all other users interested in obtaining an illegal copy of the work.

But there is a major difference between spyware and DRM software that may help. DRM software is protected by the anti-circumvention provisions of the Digital Millennium Copyright Act. These provisions prohibit circumventing access controls, but don't prohibit circumventing use controls. It is not clear whether manually removing MediaMax or XCP would be considered circumventing either type of control. Sony can certainly make a strong argument that once installed, its DRM software prevents accessing the CD audio tracks, and uninstalling the

[18] California Civil Code § 1770(a)(5).

[19] "Analog hole" refers to the fact that it is nearly impossible for DRM to prevent a user from simply recording the analog audio (or video) output of a player and then re-digitizing that recording. For example, a user of a XCP-protected CD can simply play the CD on a standard CD player, connect the analog audio output of the CD player to the line-in jack on their computer, and re-record the CD digitally using the computer.

software is circumventing an access control. If users must be given the option to refuse the installation of DRM software, and CDs are vulnerable to copying without the installation of DRM software, the solution is to make it difficult for users to live without the DRM software. This is best accomplished by including the DRM software in the operating system itself. Microsoft is planning to do just that with the next version of Windows.[20] This approach may also solve the problem of the analog hole, as copyrightholders can include "watermarks" in their works that the operating system can detect even after the work has been converted from digital to analog and back to digital.

Conclusion

Assuming that Sony could have avoided all of the legal problems that were a result of its decision to use MediaMax and XCP by more clearly disclosing what the software did and doing a bit more testing of the installation procedure, what's the point of spyware laws? More importantly, what's the point of requiring disclosure if the disclosure can be in a lengthy EULA that the vast majority of users never read anyways? Both of these questions are mute if the exemption in § 22947.3 applies to DRM software. These concerns seem to suggest that spyware legislation is ill-suited to deal with DRM software. It arguably suggests that spyware legislation is ill-suited to deal with spyware.

These issues are not confined to the single instance of MediaMax and XCP. CinemaNow, a website that sells movies that users can burn to DVD, reportedly introduces deliberate errors in

[20] See http://www.symantec.com/enterprise/security_response/weblog/2006/08/assessment_of_vista_kernel_mod.html

the DVD burning process in order to prevent copying the burned DVD.[21] TiVo has updated the firmware on its Digital Video Recorders to allow networks to flag shows so they can't be recorded or must be watched within 24 hours.[22] This de-facto broadcast flag ability was not included in the TiVos as sold, and users were not given the option to refuse this new "feature."

Just as there is an industry group devoted to defining what is and isn't spyware, which is based on what should and shouldn't be allowed, there should be an industry group defining what is and isn't acceptable for DRM software. If the software industry doesn't police itself, courts will have to decide when users are entitled to manually uninstall unwanted DRM software that they "accidentally" installed because they didn't carefully read and fully comprehend the accompanying EULA. Ruling on such technical matters is something that courts are not well-equipped to do, and decisions in individual cases will have little precedential value as technologies change rapidly.

[21] http://www.boingboing.net/2006/08/02/cinemanows_burntodvd.html

[22] http://www.zatznotfunny.com/2006-08/tivo-macrovision-and-the-stealth-broadcast-flag/