SONY COPY PROTECTION

An Interactive Qualifying Project Report

Submitted to the Faculty

of the

WORCESTER POLYTECHNIC INSTITUTE

in partial fulfillment of the requirements for the

Degree of Bachelor of Science

By

_____

Jeremy N. Lounder

_____

Brian G. Weber

9 March 2006

_____

Professor George T. Heineman, Major Advisor

TABLE OF CONTENTS

SONY DRM

THE CASE AND THE AFTERMATH

ABSTRACT

To prevent consumers from illegally copying music compact discs, Sony BMG included extended copy protection software on compact discs distributed across the globe. This project includes a case study which evaluates Sony BMG's attempts to protect its music, whether ethical, unethical or even illegal. The attention remains on laws protecting copyrights in the United States and describes the impact on all players of the music industry. The policy outlined applies practical restrictions on the future use of copy protection software.

INTRODUCTION

OVERVIEW

The compact disc first achieved mass manufacturing in 1982 through the combined efforts of Sony and Phillips. Initially the classical music industry and the audiophile community (high fidelity recordings) used the new technology (which was a significant improvement over the popular analog cassette-tape recordings and vinyl record formats at the time). The "Red Book" standard for compact disc in digital audio format (CDDA) was created by Sony and Phillips in 1980 and subsequently adopted by the Digital Audio Disc Committee. This standard outlines the data format and physical specifications of any disc that is to meet the standard. For example, the standard sampling rate of CDDA discs is 44100 samples per second for two channels (stereo audio). Also, the structure of the data on the disc is defined within the standard as well: the disc is comprised of sectors that are 2352 bytes. Discs that comply with this standard may be labeled with the CDDA logo. [37]

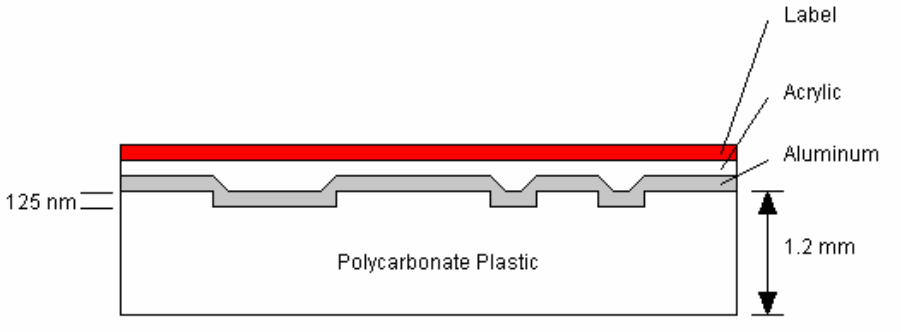

Figure 1 – Side view of a compact disc

In May of 1985, the popular Rock and Roll group Dire Straights released their album *Brothers in Arms* on compact disc, demonstrating both the quality and capacity of this new form of media. They were the first major rock group to release an all-digital recording, and this album contributed greatly to the rise of the compact disc. [4]

As time passed, the compact disc market continued to grow. By 1990, 288 million compact discs were sold in the United States [35]. During this time personal computer sales skyrocketed. By 2000, nearly fifty-four

million households (about fifty-one percent) had at least one computer [23]. The "Yellow Book" standard for Compact Disc Read-Only Memory (CD-ROM) was created in 1985 by Sony and Phillips. In 1987, John Sculley (the CEO of Apple at the time) predicted that CD-ROMs would "revolutionize the use of personal computers" [3]. The PC boom, coupled with CD-ROM technology, allowed consumers to copy or "rip" music from compact disc to the hard drive of a computer. A compact disc holds between 650 and 700 megabytes of data and a typical hard drive in 1998 only held 1 gigabyte of information [10]. The Mpeg Layer 3 (MP3) is one method used to compress tracks to a more manageable size for storage on personal computers. This standard was invented by Fraunhofer Institut Integrierte Schaltungen (the "Fraunhofer Integrated Control Institute") in 1987 [31]. MP3 is patented and thus must be licensed by its creators. This is why free alternatives such as Windows Media Audio (WMA), Ogg-Vorbis (OGG), and others have arisen over the years, but have been yet unable to match the popularity of MP3. MP3 was the first major compression technology for audio tracks, so this format is widely compatible with devices and software for playing audio.

"Sixty-two million U.S. households, or 55 percent of American homes, had a Web-connected computer in 2003, according to just-released U.S. Census data." This figure is nearly triple the 1997 figure, with Web-connected computer owners comprising just 19 percent of the population. [28]. With this rapid growth came the ability to share ripped tracks with other users and easily find desired music for download. A 2004 study on the effect of file sharing on record sales states that "Among U.S. adults at least eighteen years old, the number of downloaders has about doubled since 2000" [33]. Record labels saw this growth and concluded that these users no longer needed to purchase their own copy of CDs to get the music they wanted. Brad Buckles, the Executive Vice President of Anti Piracy at the RIAA characterized illegal downloading as follows: "The online theft of music – whether on rogue file-sharing networks or in piracy distribution groups – directly affects our ability to invest in new bands and new music that fans want to hear" [38]. For this reason, they quickly began work on means to protect CD content from illegal distribution.

Most copy protections schemes were designed to work on Windows PCs, which is a logical step considering that in 2002, 93.8 percent of desktops were running Windows [46]. Early attempts to protect CD content took the form of mixed mode discs that contained both music and data. The data portion often contained audio player software that ran automatically on Windows-based PCs. This could be circumvented easily by either disabling auto run or holding SHIFT when putting the disc in. [5]

The music recording industry began as a community to promote the concept of Digital Rights Management (DRM) to address challenges in copy protection. This technology was developed to account for the ease with which users can extract digital music from compact discs. Nearly all of the hardware methods are able to be circumvented through the use of hardware to record. If the computer can play the music, the music can be recorded with little or no quality loss. It is unrealistic for the recording industry to stop users from playing compact discs in their computers, so DRM software is the alternative. The two major examples of DRM software are the iTunes DRM using FreePlay and the Windows Media DRM employed by the resurrected Napster and others. These different methods of rights management ensure through server communication that the songs are only played on a certain number of computers, or burned onto a certain number of CDs.

PLAYERS

There are many more parties affected by this case besides Sony BMG and the consumers whose computers were compromised. The artists of the affected music (and all music) are concerned because copyright protection poses a threat to their success should users decide purchasing compact discs is too risky. Also, distributors besides Sony BMG have a vested interest in this case because in many ways the outcome of this case will define the measures they can and cannot take to protect their intellectual property. Retailers would also feel any potential harmful effects to compact disc sales, as they are responsible for the actual sale to the consumer of nearly all compact discs. Finally, the United States legislature and judiciary play an important role in this case, as they are the protectors of copyright law.

All music artists have a vested stake in the music industry, because the industry is responsible for the production and distribution of their music worldwide. The current Sony XCP copy protection fiasco has caused artists to take a step forward against copy protection on CDs. Their actions range from shipping out copies of their CDs directly to customers who have complained (as the band My Morning Jacket did) to actually speaking out against the actions of the industry. Steve Foreman of Switchfoot (one of the affected Sony BMG artists) wrote the following in a September 14 post on the band's website: "We were horrified when we first heard about the new copy-protection policy. It is heartbreaking to see our blood, sweat and tears over the past two years blurred by the confusion and frustration surrounding new technology" [20].

Distributors are an important part of the music industry because they mass produce CDs and deliver them to the stores were people can by them. Their entire income derives from selling CDs, and every time a CD is illegally obtained instead of purchased, the distributor will ship fewer CDs and thus lose money.

Retailers are also an important player in digital rights. Wal-Mart, for example, refuses to market some CDs with explicit lyrics and will only sell "clean" versions of these CDs. If copy protected CDs are dangerous to consumers, a similar situation could arise. While retailers would like to offer a large selection of music, they may opt to ban certain discs or labels if they deem the CD contents harmful.

The final players in the music industry are the consumers who spend the money which feeds the distributor and the artist. Consumers today want the ability to copy songs from CDs onto their computer, onto other computers they use, onto mix CDs, and onto portable music devices. However, with the growing resources for obtaining illegal copies of digital media, the distributors are using copy protection methods to prevent the duplication of content they sell on CDs.

Congress has been granted the power to govern intellectual property by Article I of the United States Constitution: "The Congress shall have the power…to promote the progress of science and useful arts, by

securing for limited times to authors and inventors the exclusive right to their respective writings and discoveries." Copyright law encourages artists to create by ensuring them exclusive rights to profit from their work for their entire life plus seventy years (per the Sonny Bono Copyright Term Extension Act). After this time, however, the work enters the public domain for all to enjoy.

STAKES

According to the Recording Industry Association of America (RIAA), record sales have been decreasing over the past seven years due largely in part to illegal file sharing. Cary Sherman, the president of the RIAA, characterizes the impact of illegal file sharing: "There's no minimizing the impact of illegal file-sharing. It robs songwriters and recording artists of their livelihoods, and it ultimately undermines the future of music itself, not to mention threatening the jobs of tens of thousands" [33]. According to the RIAA's statistics, record sales have fallen substantially since 2000 as shown in Figure 2; that was the year after the incredibly popular and groundbreaking music sharing service called Napster was released (www.napster.org). The RIAA claims that this is no coincidence. With millions of tracks available freely on Napster and other file sharing services, the RIAA claims people no longer need to purchase albums or singles.

This large decrease since 2000 is equivalent to about $1.8 billion in revenue [50], but whether or not it is attributable to illegal file sharing is debatable. The RIAA fails to account for legal downloads through iTunes, Rhapsody, or the newly reconstituted (and legal) Napster service, which are likely the primary cause of the decrease in singles sales and contribute to the decrease of album sales. Also, the RIAA reports the number of compact discs shipped to retailers, as opposed to the actual sales data. This data is indeed available through Nielsen's Soundscan, as this data is used to calculate the Billboard Top 100 (Soundscan.com). Critics of the music industry also blame overpriced compact discs and even a decrease in the quality of music for the decline in sales.

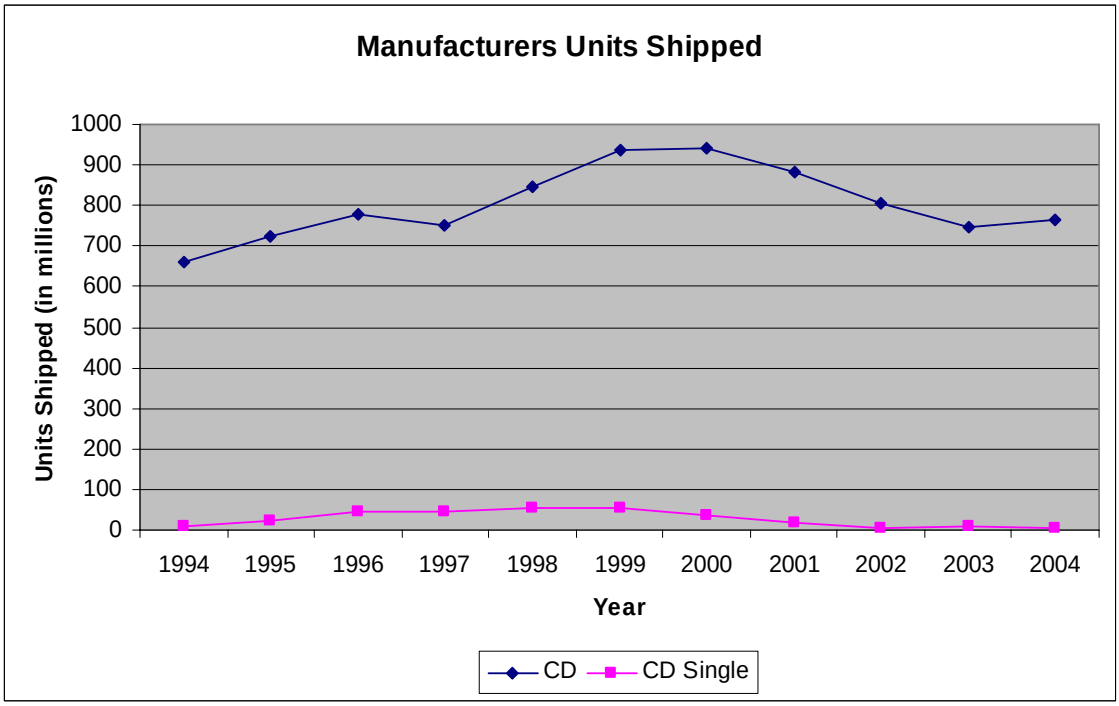

Figure 2 – Graph based on "2004 Year End Statistics" published by the RIAA [50]

The CD industry is a high stakes games with many players. One can expect that each player will take steps to maximize their profits. The music labels are putting copy protection onto new CDs to ensure consumers do not illegally copy the content. However, it is apparent that some labels may have gone too far with their current protection practices. In the next chapter we review the relevant law and court cases regarding copyrights in the United States.

LEGAL ISSUES

RELEVANT LEGISLATION

Copyright Law has existed in the United States since the founding of the republic. Under Article I of the United States Constitution, Congress is granted the power to legislate intellectual property. This power has been exercised to pass many different laws regarding intellectual properties and the rights of authors, duration of protection, and types of property protected.

COPYRIGHT ACT OF 1909

The Copyright Act of 1909 was the first major revision to copyright law after the original legislation in 1790. This law doubled the term of copyright and better defined the works protected by US copyright law. The 1790 Act provided a copyright term of fourteen years plus a possible extension of fourteen years. The 1909 Act extended the initial term to twenty-eight years and allowed an extension of twenty-eight years, thus effectively quadrupling the total possible duration of a copyright.

The Copyright Act of 1909 enabled artists to secure copyrights for "(1) literary works, (2) musical works, including any accompanying words, (3) dramatic works, including any accompanying music, (4) pantomimes and choreographic works, (5) pictorial, graphic, and sculptural works, (6) motion pictures and other audiovisual works, and (7) sound recordings" [52].

Finally, this act (as well as the 1790 Act) required that copyrights be registered and have a "©" affixed in order for the copyright to be extended. Many artists did not register their works since it was not a trivial process. This act only allowed a term of twenty-eight years for those without the means or motivation to register their work with the Copyright Office.

COPYRIGHT ACT OF 1976

The Copyright Act of 1976 updated the Copyright Act of 1909 to reflect the numerous technological advances in the intervening years. Some of these advances included television, movies, radio, and audio

recording. Clearly these new types of works needed to be protected under copyright law and the Copyright Act of 1976 set about to provide that protection. This massive piece of legislation redefined what constitutes copyrightable material, put the *fair use doctrine* into law, redefined how a work obtains copyright protection, specified the exclusive rights granted to copyright holders, and revised the scheme for expiration and renewal of copyrights.

The new act applied copyright protection to "original works of authorship fixed in any tangible medium of expression, now known or later developed, from which they can be perceived, reproduced, or otherwise communicated, either directly or with the aid of a machine or device" [48]. All of the original classes of works that were copyrightable were left intact, and architectural works were added to this list.

The fair use doctrine existed long before the Copyright Act of 1976 made it law. The court system had applied fair use for well over a century prior, dating back as far as *Evans v. Eaton (1818)*, which pertained to patent law infringement. Essentially the fair use doctrine allows owners of copyrighted works to duplicate them under certain circumstances without infringing upon the copyright. Such situations include education, archival backup, and parody.

Prior to the Copyright Act of 1976, a work needed to be published and registered with the Copyright Office to receive a copyright extension. Most authors (especially those who were not particularly notable) did not even bother to register their work because of the inconvenience. Congress determined that a better method of affixing copyright protection must be devised. Instead of requiring registration, the new Act provided copyright protection upon "fixing into a tangible medium." The Copyright Act of 1909 required that a work be published, but the new law essentially dictated that as soon as a literary work is written down or a song is recorded or written down, it is protected by copyright law. Ideas themselves are still not able to be copyrighted, but the expression of the ideas may fall under copyright protection. The only situation where

registration is required is when a lawsuit is being filed for copyright infringement, in which case the work in question must be registered with the Copyright Office.

This shift in protection requirements is one of the most important pieces of the Copyright Act of 1976. By removing the registration process and protecting works upon translation to a tangible medium, the spirit of copyright law is better upheld. Copyright protection is not intended to only be afforded to those educated and able to obtain a copyright.

The exclusive rights aspect of the Copyright Act of 1976 simply expands the 1909 legislation to include the right to produce derivative works. This addition stems from the concept of indivisibility established by the 1909 Act essentially stating that a copyright holder cannot sell the rights to part of his work, but must sell the rights to the entire work or not at all. Any person only owning partial rights to a copyrighted work was considered to be a licensee not an assignee. This was originally designed to prevent extraneous lawsuits, since only assignees and copyright owners may initiate lawsuits However, Congress decided that is was unrealistic for assigned rights to be all or nothing, so the Copyright Act of 1976 changed this. This allowed authors to give rights to derivative works, for example. [40]

The final aspect of the Copyright Act of 1976 dealt specifically with the duration of copyright protection and renewal. The 1909 act had set copyright duration at twenty-eight years with the possibility for a twenty-eight year extension. The 1976 act, on the other hand, set the duration of the copyright to be the duration of the author's life plus another fifty years. This would again be extended in the Copyright Term Extension Act.

DIGITAL MILLENNIUM COPYRIGHT ACT (1998)

The Digital Millennium Copyright Act was passed in 1998 to update existing United States copyright law to comply with international copyright treaties such as the World Intellectual Property Organization (WIPO) and provide legislation for newer forms of intellectual property not covered by the Copyright Act of 1976, specifically digital media.

One of the important sections of this legislation deals with the circumvention of copy protection. Essentially, this section covers two types of copy protection: access protection and copy protection. Access protection restricts unauthorized users from accessing the work, while copy protection prevents unauthorized users from copying the work. This is an important distinction in the legislation. The text of the legislation is as follows, with regard to access control circumvention:

> (2) No person shall manufacture, import, offer to the public, provide, or otherwise traffic in any technology, product, service, device, component, or part thereof, that--
> `(A) is primarily designed or produced for the purpose of circumventing a technological measure that effectively controls access to a work protected under this title;
> `(B) has only limited commercially significant purpose or use other than to circumvent a technological measure that effectively controls access to a work protected under this title; or
> `(C) is marketed by that person or another acting in concert with that person with that person's knowledge for use in circumventing a technological measure that effectively controls access to a work protected under this title.

The language of the section on copy protection circumvention is nearly identical, with "access" replaced with "protects a right of a copyright owner under this title". This part of the legislation is designed to prevent developers and inventors from creating software and hardware for the sole or primary purpose of circumventing copy protection. This is important in the digital age because software is no longer just distributed in retail stores; it is also distributed over the Internet. This increased availability of software allows developers to post their work on the Internet, which is largely unregulated. This section of the DMCA allows corporations and other copyright holders some recourse against individuals and companies facilitating copyright infringement.

This section of the DMCA also provides some specific instances where circumventing copy protection is legitimate. It is important to note that the text of the bill itself states: "Nothing in this section shall affect rights, remedies, limitations, or defenses to copyright infringement, including fair use, under this title." Despite this intent, there is no provision for allowing personal archival backups, for example. The exceptions

provided are for non-profit libraries, archives, educational institutions, law enforcement or government activity, reverse engineering, encryption research, security testing, and computer maintenance. This legislation also provides an exception for access restriction to minors on the Internet and for the protection of personally identifying information.

The most interesting of the exemptions under the DMCA is reverse engineering. This provision allows a user who has legal right to use a piece of software to reverse engineer for the "sole purpose of identifying and analyzing those elements of the program that are necessary to achieve interoperability of an independently created computer program with other programs, and that have not previously been readily available to the person engaging in the circumvention." This provision allowed the creators of OpenOffice (an open-source free suite of software comparable to Microsoft Office), for example, to reverse engineer Microsoft Office to determine the format that files are saved in since this allowed interoperability between Office and OpenOffice.

The exception for personally identifying information allows users to circumvent copyright "a technological measure that effectively controls access to a work protected under [the DMCA]" under the condition that the user is attempting to disable a mechanism by which the measure collects personal information. The program or device must not either inform the user of the collection or allow the user to disable the collection. This provision allows users to protect their personal information from unauthorized dissemination or collection.

This legislation also protects Internet Service Providers (ISPs), granting them limited liability for the traffic on their networks. This essentially frees ISPs from having to filter traffic and set up regulations disallowing certain protocols and services, for example. It is important however, that the following conditions are met:

> `(1) the transmission of the material was initiated by or at the direction of a person other than the service provider;
> `(2) the transmission, routing, provision of connections, or storage is carried out through an automatic technical process without selection of the material by the service provider;

> `(3) the service provider does not select the recipients of the material except as an automatic response to the request of another person;
> `(4) no copy of the material made by the service provider in the course of such intermediate or transient storage is maintained on the system or network in a manner ordinarily accessible to anyone other than anticipated recipients, and no such copy is maintained on the system or network in a manner ordinarily accessible to such anticipated recipients for a longer period than is reasonably necessary for the transmission, routing, or provision of connections; and
> `(5) the material is transmitted through the system or network without modification of its content. (HR 2281)

This essentially means that as long as ISPs maintain ignorance of the activities that go on and have "an automatic technical process" for routing (which they all do), they are not liable for damages. However, there is a stipend to this, which is that they must comply with all legitimate claims by copyright holders and their representatives to identify a user on their network that is infringing on copyright.

This legislation provides the added ability of copyright holders to request a subpoena to identify an infringer. The request for subpoena must contain (among other things) "a sworn declaration to the effect that the purpose for which the subpoena is sought is to obtain the identity of an alleged infringer and that such information will only be used for the purpose of protecting rights under this title." This provision is to ensure that subpoenas are not obtained under the guise of protecting copyrights and then used for other purposes. Additional information is provided by the legislation regarding the subpoena:

> `(3) CONTENTS OF SUBPOENA- The subpoena shall authorize and order the service provider receiving the notification and the subpoena to expeditiously disclose to the copyright owner or person authorized by the copyright owner information sufficient to identify the alleged infringer of the material described in the notification to the extent such information is available to the service provider.
> `(4) BASIS FOR GRANTING SUBPOENA- If the notification filed satisfies the provisions of subsection (c)(3)(A), the proposed subpoena is in proper form, and the accompanying declaration is properly executed, the clerk shall expeditiously issue and sign the proposed subpoena and return it to the requester for delivery to the service provider.
> `(5) ACTIONS OF SERVICE PROVIDER RECEIVING SUBPOENA- Upon receipt of the issued subpoena, either accompanying or subsequent to the receipt of a notification described in subsection (c)(3)(A), the service provider shall expeditiously disclose to the copyright owner or person authorized by the copyright owner the information required by the subpoena, notwithstanding any other provision of law and regardless of whether the service provider responds to the notification.

> `(6) RULES APPLICABLE TO SUBPOENA- Unless otherwise provided by this section or by applicable rules of the court, the procedure for issuance and delivery of the subpoena, and the remedies for noncompliance with the subpoena, shall be governed to the greatest extent practicable by those provisions of the Federal Rules of Civil Procedure governing the issuance, service, and enforcement of a subpoena duces tecum [A command to a witness to produce documents]. [8]

The limited liability for Internet Service Providers (ISPs) provided by this legislation comes at the cost of this subpoena section, which has allowed the RIAA and other corporations to track down and sue individual users for their infringements. [8]

COPYRIGHT TERM EXTENSION ACT (1998)

The Copyright Term Extension Act (CTEA) of 1998 was proposed to synchronize United States copyright duration with those of the European Union to protect the rights of United States copyright holders. This act was introduced with the support of Disney and other corporations that had old copyrights that were due to expire. These corporations still profited a great deal from the ownership of these copyrights and contended that they should continue to own the rights.

The effect of this bill was simple: copyright terms for individual authors were extended to the life of the author plus seventy years and ninety-five years for corporate authors. This was an increase of twenty years for each. This means that no currently copyrighted works will enter the public domain until 2019 at the earliest. [6]

FAIR USE

The fair use doctrine defines certain circumstances under which copyright protection can be violated without constituting infringement. "In its most general sense, a fair use is any copying of copyrighted material done for a limited and 'transformative' purpose such as to comment upon, criticize or parody a copyrighted work." Additionally, under the Copyright Act of 1976, this doctrine was put into law and expanded to include

archival backup and educational use. This doctrine is an important part of intellectual property law, as it ensures that copyright law does not inhibit progress and that the spirit of the law is upheld.

"A parody is a work that ridicules another, usually well-known work, by imitating it in a comic way". In most cases, courts will allow a substantial amount of the original work to appear, since this is necessary to accomplish the imitation that is the basis of parodic work.

Commentary or critical works are allowed to contain copyrighted material as well. For example, a review of a book may contain quotes from the book without the author's consent. This is beneficial to the public because the review is substantiated by the parts of the work.

Ultimately, the fair use doctrine is subject to the opinion of the Court. There are no set rules for fair use, since every case is different and must be treated differently. According to the Copyright Act of 1976, the following items should be considered when evaluating fair use:

1. The purpose and character of the use, including whether such use is of a commercial nature or is for nonprofit educational purposes;
2. The nature of the copyrighted work;
3. The amount and substantiality of the portion used in relation to the copyrighted work as a whole; and
4. The effect of the use upon the potential market for or value of the copyrighted work.

In general, very little copied material or a small or negligible economic effect is more likely to fall under fair use protection.

Fair use provides the flexibility that copyright law cannot by putting the power to decide in the hands of the courts. This is important to deal with the wide variety of cases that arise out of copyright law. [17]

SONY CORP. V. UNIVERSAL CITY STUDIOS, INC. (1984)

This 1984 ruling is a landmark case in the history of court copyright law because the ruling established an important guideline for determining if creators of technology that may be used for copyright infringement are liable for such infringement. Universal City Studio was attempting to hold Sony responsible for the damages caused by infringement of users with the help of the Betamax video tape recorder (VTR). Universal held that Sony devices allowed users to record television programs to which Universal had copyrights to and replay them in a public viewing, which was an infringement of copyright. Universal opted not to go after the infringing users, but Sony to attempt to cease the production of these devices. Sony contended that the use of VTRs in the home was perfectly legal, and thus they were not liable for contributory infringement.

The Court's ruling on this case is a monumental one, as it would be applied time and again to cases regarding contributory copyright infringement, that is, cases where technology played a role in copyright infringement. The Supreme Court contended that the primary use of these VTRs was the act of "time-shifting". This refers simply to the automated or manual recording of a television program so that one may privately view the program at a more convenient time. There are some important aspects of time-shifting that the Supreme Court noted the following:

> There is no likelihood that time-shifting would cause nonminimal harm to the potential market for, or the value of, respondents' copyrighted works. The VTR's are therefore capable of substantial non-infringing uses. Private, noncommercial time-shifting in the home satisfies this standard of non-infringing uses both because respondents have no right to prevent other copyright holders from authorizing such time-shifting for their programs, and because the District Court's findings reveal that even the unauthorized home time-shifting of respondents' programs is legitimate fair use. [45]

Also, it is important to note the following observation of the court: "The Copyright Act does not expressly render anyone liable for infringement committed by another" [45]. This is in stark contrast to patent law, in which inducing patent infringement makes one liable. The Court ruled in favor of Sony saying that Sony was not liable for contributory infringement.

Thus, the famous *Sony* test was conceived. Under this precedent, a product is not liable for contributory infringement if it "is capable of substantial non-infringing uses" [45]. The dissenting members of the Court pointed to the fact that this test is overly vague and unclear as to what qualifies as "substantial" and that nearly any device may qualify under this standard. Despite this fact, the *Sony* test has been used since the 1984 ruling.

ELDRED V. ASHCROFT (2003)

This case was brought before the Supreme Court by opponents of the Copyright Term Extension Act of 1998. The plaintiff was Eric Eldred, who ran an Internet-based publisher of public domain works. He was backed by a number of publishers, libraries, and associations who used public domain work. The United States government was the defendant in this case, backed by the Motion Picture Association of America, Recording Industry Association of America, American Society of Composers, Authors, and Publishers, and Broadcast Music Incorporated. These groups stood to gain a great deal by copyright term extension, as this meant they could profit from copyrighted works for longer. The plaintiff stated the following reasons for challenging this legislation:

> That by retroactively extending copyright terms, Congress had violated the requirements of the Constitution's Copyright Clause, which gives Congress the following power:
>
> "To promote the Progress of Science and useful Arts, by securing for limited Times to Authors and Inventors the exclusive Right to their respective Writings and Discoveries"
>
> Plaintiffs argued that by reading this formulation so as to allow for any number of retroactive extensions, Congress could in practice guarantee an unlimited period of copyright protection, thus thwarting the intent of the clause.
>
> That any copyright law must be subject to scrutiny under the First Amendment, thereby insuring a balance between freedom of speech and the interests of copyright.
>
> That the doctrine of public trust requires the government to show a public benefit to any transfer of public property into private hands, and that the CTEA violates this doctrine by withdrawing material from the public domain. [15].

Based on these claims, the plaintiff stated that the CTEA should be deemed unconstitutional and removed from law.

Essentially, the courts at every level rejected every claim of the plaintiff. Congress, the Court argued, had the power to extend terms of copyright as long as each extension was a finite number. On the second claim, the Court disagreed that the First Amendment was applicable to these situations and thus this consideration was not necessary. The third argument was dropped at the Appeals Court level and thus was not directly addressed by the Supreme Court.

This ruling meant that the CTEA remained in effect. Additionally under this ruling, the Court confirmed the ability of Congress to extend the terms of copyrights to the coveted "forever minus one day" duration proposed by copyright proponents. This would be possible as long as the extensions continued to happen in finite increments. This ruling squashed most of the legal opposition to the Copyright Term Extension Act.

LEXMARK INTERNATIONAL, INC. V. STATIC CONTROL COMPONENTS, INC. (2003)

This case is a direct attempt to use the copyright circumvention section of the DMCA to protect a design. In this case, Lexmark (a leading manufacturer of printers and ink/toner cartridges) claimed that Static Control Components (a manufacturer of toner cartridge parts) violated the copyright protection circumvention section of the DMCA. To protect their toner cartridge design, Lexmark had added a handshake mechanism between cartridge and printer. This mechanism consisted of two chips on both the printer and toner that monitor toner levels ("Toner Loading Program") and control paper feeding and other operations of the printer ("Printer Engine Program"). Lexmark implemented a secret code exchange, without which the printer would not be able to access either the toner monitor or the printer controller and thus the printer would not function properly. To maintain their product, Static Control Components reverse engineered the handshake mechanism and provided a similar mechanism on their cartridges to allow functionality in Lexmark printers in addition to a copy of the Toner Loading Program provided by Lexmark. This reverse engineering was the basis for Lexmark's claim that Static Control Components violated the DMCA.

Additionally, Lexmark had a program in place called the "Prebate" program, which allowed companies to purchase cartridges at a reduced price under the condition that they return the used cartridge to Lexmark after use. This allowed Lexmark to refill the cartridges and resell them as recycled cartridges. Lexmark's toner monitoring program did not allow users to refill their own cartridges. Essentially, the chip that Static Control (the SMARTEK chip) developed allowed users to purchase the cartridges from Lexmark under the Prebate program, but instead of returning the cartridges they could refill them.

Lexmark argued that Static Control has "infringed and continues to infringe Lexmark's copyrights in the Toner Loading Program by manufacturing and selling SMARTEK microchips that contain unauthorized, identical copies of Lexmark's copyrighted Toner Loading Program." Also, Lexmark claims that Static Control violated the anti-circumvention section of the DMCA, claiming that the appropriate measure were in place to protect the copyright, but Static Control was able to circumvent them.

The Sixth Appeals Court ruled in favor of Static Control Components, thus overturning the ruling by the lower court. The Sixth Appeals Court determined that the Toner Loading Program was not in itself copyrightable, since it was so simple and essentially contained a formula for estimating the amount of toner in the printer. The Court also determined that duplication of this code was necessary to achieve compatibility.

The most important aspect of the case, however, was the application of the DMCA by Lexmark. This application of the DMCA was rejected because the Court determined that although there was an authentication mechanism in place, it was entirely possible to bypass this authentication and read the printer software directly from the internal RAM of the printer. Essentially this ability nullified Lexmark's claim because the DMCA only affords protection if the protection "effectively controls access to a work." [27].

METRO-GOLDWYN-MAYER STUDIOS INC. ET AL. V. GROKSTER, LTD., ET AL. (2005)

The two main parties involved in this case are MGM Studios and Grokster, ltd. MGM Studios is "an independent, privately-held motion picture, television, home video, and theatrical production and distribution company" (MGM.com). Grokster, on the other hand, was a company that developed and distributed peer-to-peer file sharing software. Going to the Grokster website reveals the company's fate:

> "The United States Supreme Court unanimously confirmed that using this service to trade copyrighted material is illegal. Copying copyrighted motion picture and music files using unauthorized peer-to-peer services is illegal and is prosecuted by copyright owners. There are legal services for downloading music and movies. This service is not one of them" (Grokster.com).

Essentially, the technology in question is software that creates and maintains a peer-to-peer network. Peer-to-peer protocols are not a new concept, but have just recently found application with file sharing over the Internet due to the increased prominence of broadband connections and the explosion of the Internet. In a peer-to-peer network, each computer on the network acts as both a client and a server, both sharing and downloading files. This setup is ideal for Internet file sharing because for most connection types downloading is substantially faster than uploading. A peer-to-peer network exploits the great number of available hosts to provide faster download speeds to all users by downloading from multiple sources simultaneously.

This case divided the software and entertainment industries. Software companies contended that if Grokster were to be held liable, it would inhibit innovation and technological progress. They also feared that this ruling would overshadow the *Sony* ruling and there would be more restrictions placed on legal software that could be used for copyright infringement. The RIAA and MPAA sided with MGM and the entertainment giants, claiming that this was a necessary step to ensure the balance that the *Sony* ruling provided.

In this case, MGM and twenty-seven other entertainment corporations sought to close the operations of Grokster and Streamcast (the company that created and distributed Morpheus) citing that the software they had developed facilitated copyright infringement. Grokster and Streamcast contended that there were many

legal applications for peer-to-peer software and for this reason the software was protected under the *Sony* test established in the case of *Sony Corp. of America v. Universal City Studios, Inc.* This test dictates that technologies that facilitate copyright infringement may only be safe from litigation if they have significant non-infringing applications. Grokster contended that their software passed this test.

MGM and the other entertainment companies contended, however, that the quantity of non-infringing uses of the software was insufficient to qualify for protection under the *Sony* test. Also, MGM insisted that Grokster was profiting greatly by actively inducing users to engage in copyright infringement that this in itself should make them liable. They also contended that it was entirely possible for Grokster to actively combat copyright infringement, but that the company failed to do so.

In the end, the Court sided with MGM and determined that Grokster's software indeed did not have sufficient legal non-infringing uses to be protected by the *Sony* ruling and that Grokster was indeed liable for the infringement occurring as a result of the software they distributed. For liability reasons, Grokster closed its doors, vowing to return to the market with a legal alternative. At the very least, companies will attempt to do a better job of advertising the legal and legitimate uses of their software so as not to be caught up in active inducement of copyright infringement. [42]

With a detailed understanding of the current safeguards given to the copyright owners and the rights given to users of copyrighted material, we can delve further into the case at hand. This case deals with the fine balance between protecting the right of the copyright owner to copy and distribute the protected material and the end user's right to create archival backups and to use the material for purposes covered by Fair Use. The current legislation under consideration is discussed in the policy outline section later in this document.

CASE STUDY: SONY XCP

THE SOFTWARE

Sony BMG's most recent attempt at copy-protection is a software package they call extended copy protection (XCP). XCP software is intended to limit the end user's ability to use the music they purchase, by restricting how many times it can be copied and monitoring when the music is accessed.

When you first insert a CD with Sony's XCP software on it into your computer you are presented with Sony's End User License Agreement (EULA). The EULA tells you that in order to access the music contained on the CD you are required to "install a small proprietary software program … onto your computer. The software is intended to protect the audio files embodied on the CD, and it may also facilitate your use of the digital content. Once installed, the software will reside on your computer until removed or deleted. However, the software will not be used at any time to collect any personal information from you, whether stored on your computer or otherwise" [44].

This software maintains a list of what songs you have copied to your hard drive from protected CDs and how many times you have copied each song to a blank CD or portable media player. While the XCP software remains active, this list is used to prevent the user from copying any song more than three times. Once a song is copied a third time, the software disables the ability to copy that song, but the song remains playable on the computer.

TIMELINE

The following timeline starts on August 1, 2003, when Sony BMG first admitted they started releasing copy protection software on CDs. The timeline continues until February, 2006 and notes each significant event which directly relates to Sony BMG's XCP software.

PAST

August 1, 2003: Sony BMG began to market and sell compact discs (CDs) containing copy protection software. The copy protection software allows a consumer to copy music from the CD into a digital file on their computer. The digital file could then be used by the consumer for specific authorized uses, such as copying to approved portable devices or onto no more than three blank CDs. [25]

June 1, 2005: Sony BMG Music Entertainment had sold more than one million copies of CDs which contain technology from First 4 Internet (F4I), a company in the United Kingdoms which specializes in software to prevent piracy. F4I created a software package known as XCP for release on Sony BMG CDs. The XCP software is designed to limit the number of copies consumers are allowed to make of protected disks. Sony BMG did not release the titles of the CDs which contain this XCP software. Sony BMG planned for a large portion of CDs they market and sell to have some form of copy protection software. [38]

OCTOBER 2005

October 31, 2005: Mark Russinovich, of Sysinternals, scanned his system with a product designed by Sysinternals called RootKitRevealer (RKR). Russinovich discovered that his system had been infected by some form of rootkit software. Using RKR, Russinovich determined the name of the driver which was running the rootkit software on his system. By simply renaming that driver and rebooting his computer, he disabled the cloaking effect of the rootkit. Once the cloaking technology was removed, he was checked the digital signatures of the files which were being cloaked and discovered they were produced by F4I.

After realizing the connection between F4I and Sony BMG, Russinovich remembered he had just bought a Van Zant CD which had been released by Sony BMG. He inserted the CD and watched as previously cloaked processes on his computer came to life. This confirmed that the CD he had purchased was linked to F4I's software, and therefore Sony BMG was responsible for installing a rootkit on millions of consumers' computers. [41]

November 2, 2005: Sony BMG and F4I released a patch for their XCP software, with the following announcement: "This Service Pack removes the cloaking technology component that has been recently discussed in a number of articles published regarding the XCP Technology used on Sony BMG content protected CDs. This component is not malicious and does not compromise security. However, to alleviate any concerns that users may have about the program posing potential security vulnerabilities, this update has been released to enable users to remove this component from their computers." [12]

November 3, 2005: Ed Felten, a professor of Computer Science and Public Affairs at Princeton, did a short analysis of the Service Pack released by Sony BMG. He contested that this patch is much too large for its only purpose to be disabling the cloaking technology. As Russinovich proved, the cloaking technology could be disabled by simply renaming the rootkit's driver file, which could be done in only a few lines of code, and a considerably smaller patch. The patch contained new copies of nearly every file in the rootkit along with several new files. [18]

November 4, 2005: Representatives from Sony BMG interviewed with National Public Radio (NPR). Sony executives objected to the use of the terms, "spyware, malware, and rootkit," when referencing their XCP software. However, their software is a rootkit by definition and design. During the interview, Thomas Hesse, President of Global Digital Business at Sony BMG, said, "Most people, I think, don't even know what a rootkit is, so why should they care about it?" However, several years ago most people did not know what a Trojan virus was, but Trojan viruses are some of the most destructive viruses on the Internet. [47]

November 11, 2005: Sony BMG vowed to stop shipping CDs with XCP software installed. Sony BMG also stated it still believes it has the right to prevent customers from illegally burning copies of its CDs and made the following statement: "We also intend to re-examine all aspects of our content protection initiative to be sure that it continues to meet our goals of security and ease of consumer use." [12]

November 12, 2005: Matti Nikki, a researcher from Finland, discovered that Sony BMG's uninstaller, from November 3, does much more than Sony BMG stated. To download the uninstaller, you first had to accept a Sony ActiveX control into your system. This ActiveX control is designed in such a way that once you install it, scripts from any website you view in the future can use the functions which it includes. This control contained approximately 23 functions, including ones that allow foreign scripts to see if you are logged in as an administrator, install or uninstall software updates, and reboot your computer. There are other functions named GetAlbumArtist, GetAlbumName, GetMaxBurnCount, GetCurrentBurnCount, and IsContentOwnerValid. These names seem to be self explanatory; they appear to allow foreign scripts which you view in any browser with ActiveX installed to see the status of all digital music on your computer. [32]

November 14, 2005: Felten and an associate, J. Alex Halderman, confirmed Nikki's report on the Sony BMG uninstaller. They elaborated about what the uninstaller actually does. The ActiveX control was written by F4I and is called CodeSupport. CodeSupport remained active on your system after you are done running the uninstaller on Sony BMG's site, and is flagged safe for scripting by other websites. "One thing CodeSupport can be told to do is download and installed code from an Internet site. Unfortunately, CodeSupport doesn't verify that the downloaded code actually came from Sony or First4Internet," write Felten and Halderman. This means that any website author can package a malicious program within their website, and if you ever view that website with Internet Explorer, after having installed CodeSupport, the malicious code will be installed automatically. [19]

November 14, 2005: Sony BMG Music Entertainment announced that it will pull some of the more popular CDs which contain XCP from store shelves. Sony BMG stated that more than twenty titles were released with XCP software, more than 4 million CDs of those titles were produced, and approximately 2.1 million have already sold. Sony BMG planned to release details of a consumer exchange program later in the week. However they still planned for all major releases in 2006 to have some form of copy protection software. [21]

November 14, 2005: James Michaelson and Ori Edelstein filed a complaint against Sony BMG Music Incorporated and F4I. The complaint claimed that Sony BMG and F4I "crafted an anti-burning scheme that would make permanent and irreversible alterations to the core windows operating system which could later be utilized by hackers or Sony to take control of the users' computer without the users' knowledge" and "have taken concerted action to cover up their actions under the guise of trying to fix the problem." [30]

November 15, 2005: Days after the initial release of the XCP uninstaller, Sony issued the following statement: "We currently are working on a new tool to uninstall First4Internet XCP software. In the meantime, we have temporarily suspended distribution of the existing uninstall tool for this software. We encourage you to return to this site over the next few days. Thank you for your patience and understanding." However, Sony failed to admit that the original uninstaller caused more security problems than it fixed which leaves consumers who have not read Felten and Halderman's report vulnerable to attack. [12]

November 19, 2005: Sony BMG announced that they will be exchanging all CDs containing XCP software for CDs without the XCP software. Sony BMG will also provide MP3 files of the music on the affected CD at no cost, if the consumer chooses. [4]

November 20, 2005: Mark Lyon created a website, http://www.sonysuit.com/, where interested consumers can view the status of law suits against Sony BMG and F4I. Lyon also filed an individual suit against Sony BMG alleging, "Breach of Warranty, Fraud, Invasion of Privacy, Negligence, Computer Fraud and Trespass, Denial of Access, Use of Access, and an Offense against Computer Equipment. It seeks: money damages, interest, punitive damages, cost of suit, and whatever else the court deems proper." [29]

November 21, 2005: Greg Abbot, Texas Attorney General sued Sony BMG Music Entertainment for installing cloaking software on consumers' computers without their knowledge. Sony BMG defended the

XCP software by saying the software prevents unlimited copying and does not gather personal information about the consumer. The Attorney General's investigation revealed some interesting facts, including that the XCP software runs on affected computers even after Sony BMG's media software is disabled. The Attorney General called into question the true nature of this software because it never goes into an idle or off state on a consumer's computer. Citing the "Consumer Protection against Spyware Act of 2005", the Attorney General sought civil penalties of $100,000 for each violation as well all attorneys' fees and investigative costs. [34]

November 21, 2005: Ben Edelman, a security researcher, monitored the activity of the XCP software. Apparently every time a user attempts to play music from a CD in Sony BMG's media player the media player sends a request to Sony BMG's website. This request is normally answered with a file which contains no pertinent information. Edelman redirected the address of Sony BMG's site to his computer, and set up a script which would respond to requests the same way as Sony BMG's site. However, instead of returning an empty page, Edelman wrote a small warning message stating the current CD is use was under recall, and that the user should contact Sony BMG to get more information. Within a matter of minutes, Edelman had setup a warning system which would get information about the recall and exchange program out to every consumer who had purchased a XCP CD and is connected to the Internet. In the last 21 days, Sony BMG had put in no effort to deploy this strategy. [14]

November 24, 2005: F4I had taken down their original web page, which detailed the company's products and activities. They replaced it with a simple page containing a brief description of the company and contact information. [12]

November 29, 2005: Eliot Spitzer, New York Attorney General, started an investigation into Sony BMG's actions. First, he sent out undercover investigators to purchase CDs from the list of XCP CDs published by Sony BMG. Weeks after Sony BMG's recall, these CDs still stock the shelves in several retail outlets

throughout New York. Spitzer had not yet filed suit against Sony BMG, but encouraged consumers not to buy affected CDs, and encouraged stores to pull the CDs from the shelves and send them back to Sony. [22]

DECEMBER 2005

December 1, 2005: Judge Naomi Reice Buchwald signed an order which consolidated all litigation filed in or transferred to the Southern District of New York jurisdiction, which has already been filed, or will be filed in the future, which involve the same or similar legal issues. [49]

December 6, 2005: Sony BMG released a new uninstall tool for the XCP software. This tool gave the consumers the option to either completely uninstall the XCP software or to just remove the cloaking technology from the software. Sony BMG also included the following notice, "For users who have previously uninstalled XCP software using the uninstaller made available prior to November 18, 2005, we recommend that you run the currently available uninstaller, to eliminate a potential security vulnerability presented by the earlier uninstaller that was brought to our attention." [12]

December 21, 2005: Judge Buchwald extended the time given for First 4 Internet to reply to the complaint until January 18, 2006. [49]

December 28, 2005: Michaelson and the plaintiff's from other consolidated litigations filed a motion for approval of a Class Action Settlement. The Settlement indicated Sony BMG will take the following actions: Stop making CDs with XCP software; Recall all XCP CDs; provide software to remove the XCP software from infected computers; make any available fixes readily available to consumers; make changes to all copy protection practices in the next two years; waive some provisions of the EULA included with the XCP CDs; not collect personal information about the users of XCP CDs; and, provide additional benefits to the consumers who purchased XCP CDs. [49]

JANUARY 2006

January 5, 2006: Mark Lyon filed a complaint against Sony BMG which charges Breach of Implied Warranty or Merchantability, Fraud, Invasion of Privacy, Negligence, Computer Fraud and Trespass, Offense Against Computer User – Denial of Access, Offense Against Computer User – Use of Access, and Offense Against Computer Equipment. Lyons demands judgment from Sony BMG for damages, interest, punitive damages, legal costs, and any other relief deemed proper by the Court. [29]

January 6, 2006: Judge Buchwald signed a hearing order to review and possibly finalize the settlement agreement in the Sony BMG case. The hearing order dictates that any person who does not want to be included in the Settlement Class must submit a request for exclusion no later than May 1, 2006. A temporary restraining order was included which prevents anyone who has not submitted a request for exclusion from "filing, commencing, prosecuting, maintaining, or intervening in any claim, lawsuit, arbitration, administrative, regulatory, or other proceeding arising out of" Sony BMG's XCP software. The hearing ordered will take place on May 22, 2006. [49]

January 23, 2006: Lyon filed a Request for Exclusion from the Settlement Class and Release from the Temporary Restraining Order. Lyon requested this exclusion to proceed with his motion filed on January 5, 2006, because he is "unable to actively participate in the litigation pending before the Court…in a manner which would allow this court to adequately address his injury and damages." [29]

January 27, 2006: Frederick D. Cooke, Jr. filed a notice of appeal to the United States District Court of Appeals for the Second Circuit for the Hearing Order issued on January 6, 2006. The specifics of the appeal were not included in the notice. [27]

FEBRUARY 2006

February 1, 2006: An amendment to the existing Class Action Settlement Agreement was submitted by Sony BMG and approved by Judge Buchwald. [49]

INDIVIDUAL IMPACT

Sony's XCP software was primarily designed by a United Kingdom company, First 4 Internet (F4I). The rootkit portion of the XCP software could have prevented many users from detecting and preventing potentially debilitating viruses and malware from being installed on their computer systems. On November 11, 2005, Sophos, a computer security firm, discovered a virus which was intended to abuse Sony BMG's rootkit software. The virus was to be spread through an e-mail titled "Photo Approval Deadline" and went by three names, "Stinx-E Trogan," "Breplibot," and "Ryknos." The virus was designed to open a backdoor into the infected machines and try to download more dangerous code from the Internet. However, a bug in the first variant of this virus prevented it from executing correctly. More recent versions of the virus appear to have fixed this defect. So far the damage from this virus is though to be very low [54]. Although no known viruses had wide spread success exploiting the XCP rootkit, the security hole could have been used to cause irreparable damage to data and programs on any computer where a XCP CD had been used. The rootkit also reports usage information back to Sony BMG, and automatically installs updates from F4I. [41]

Mark Russinovich, who first released his discovery of the rootkit software, made an attempt at removing the software from his computer. Since software his organization, Sysinternals, had already written revealed the exact file which was running the rootkit software, Russinovich simple renamed that file so that the rootkit software could no longer be loaded when the computer boots. After rebooting the infected machine, Russinovich ran a search for any files, processes, or registry entries with the 'sys' tag which means they were previously cloaked by the rootkit. He found several running processes including one 'sysDRMServer.exe' which is labeled "Plug and Play Device Manager." He believes this process is intentionally mislabeled to make the casual user think it is an integral part of the Windows operating system. He quickly linked this process directly to Sony BMG's media player and then found that even when the media

player isn't running, the DRM Server is spending expensive computer resources to monitor other running process and open files. Every two seconds the DRM Server executes a scan which queries the running processes for: "basic information about the files, including their size, eight times each scan." [41]

Russinovich continued his attempts to completely uninstall the software from his computer by deleting all driver files affiliated with the XCP software, their corresponding registry entries, and manually stopped all running services which originated from the XCP software. He rebooted his system again. Upon logging into Windows, the first thing Russinovich noticed was that his CD drive was missing from Explorer. He found this was because the XCP software had added a filter to the default Window's CD drivers, and since the software was now missing, Windows could not run the CD drive on the modified drivers. The next step Russinovich takes to finish the manual removal ventures into an area where only a seasoned Windows expert could know how to proceed. The only way to remove the filter is by removing the entry corresponding to that filter from the registry. These changes to the registry can only be made by the Local System account, which a user cannot log into directly. Russinovich had to use a Windows tool, called PsExec, to run the registry editor as the Local System account. He then removed the filters and rebooting his system. At this point he believed the system is finally XCP free. [41]

By leaving the XCP software installed on a computer, users open themselves up to a security hole and are constantly wasting computer resources on the DRM Server which is monitoring all system activities. By making a manual attempt to uninstall the XCP software manually, users can damage their system or leave components like the CD drive inoperable. [41]

GLOBAL IMPACT

Dan Kaminsky, an independent internet security researcher, has performed a world-wide investigation on how extensive the reach of Sony BMG's XCP software has been. He cites a research paper by Luis Grangeia, "DNS Cache Snooping", which introduces the idea that DNSs around the globe are externally testable. This

means that anyone, anywhere, can ask a DNS if it has recently witnessed a query for a specific internet address, assuming they have a list of DNSs. [26]

Kaminsky has compiled a list of approximately three million DNSs. His study asked those DNSs if they had witnessed queries for either Sony BMG's XCP address or First4Internet's updater address. He found that well over five-hundred thousand servers had witnessed a call to one or both of those addresses. Another three-hundred and fifty thousand servers which reported they had seen these calls had to be ignored because they use recursive reporting. This means that they checked their own cache as well as the cache of servers near them. [26]

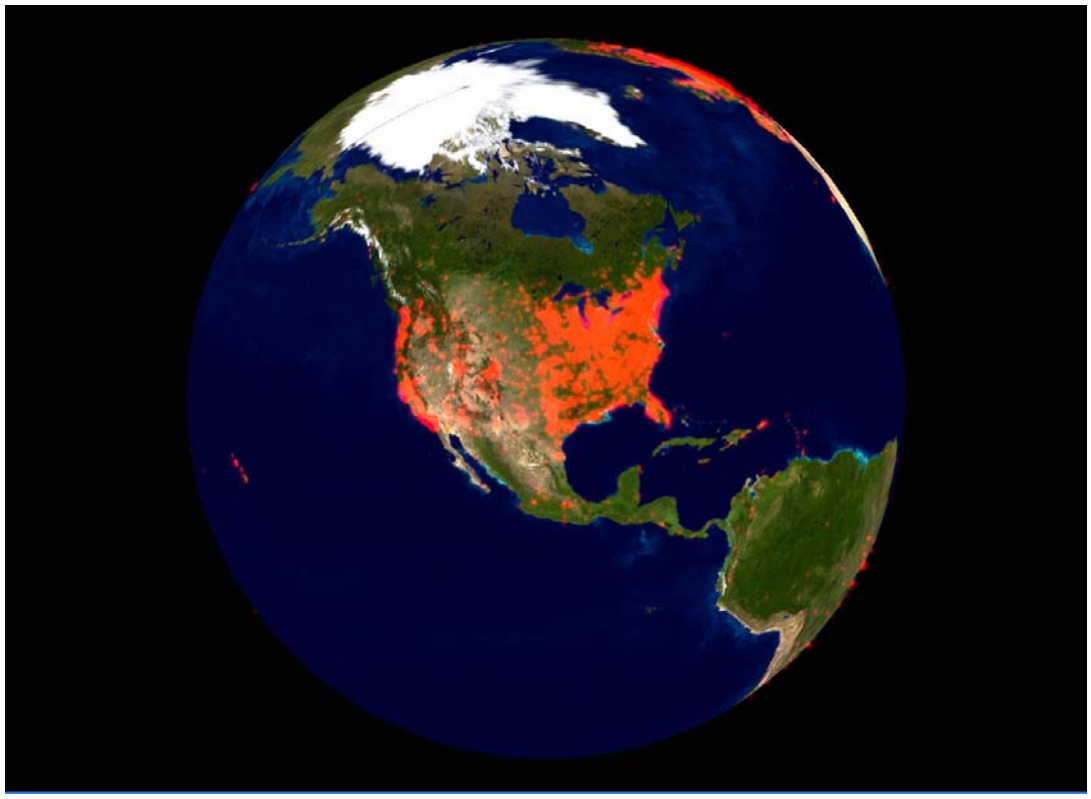

Figure 3 - This diagram is a compilation of Kaminsky's data. Each dot of orange corresponds to a positive result from a DNS.

FUTURE POSSIBILITIES

The states of New York and Florida both have investigations in progress which are looking into the issues concerning Sony BMG's XCP software. The Attorney Generals of both States have yet to file any suits or

charges against Sony BMG. The settlement agreement in the *Michaelson v. Sony BMG* case states the involved parties expect that "Sony BMG will have entered into an enforceable, nationwide agreement resolving one or more of the Government inquiries…(which) include, at least, restrictions on Sony BMG's future conduct" with the Attorney General of New York. [49]

May 1 and 22, 2006 will be important dates for people across the United States who purchased XCP CDs. On May 1, the injunction in the Hearing Order will take full effect, and people will no longer have the option of filing individual complaints against Sony BMG. The Fairness Hearing will take place on the May 22 and the Settlement Agreement could be finalized. If it does, Sony BMG will have a limited amount of time to setup the Incentive program.

The individual lawsuits against Sony BMG are still a very important factor in the continuation of the Settlement Agreement. Mark Lyon's request for exclusion from the Temporary Restraining Order was approved, and his lawsuit will be continuing. His claims have the capability to result in damages much greater than the Incentive Program proposed in the Michaelson case, which could encourage many other people to request exclusion from the Class Action Settlement and file individual actions. Cooke also has a notice of appeal filed with the US Court of Appeals. At this time the actual appeal has not been filed or made public. If his appeal is filed and approved, the Fairness Hearing could be delayed and the Temporary Restraining Order could be rescinded. A delay in the Fairness Hearing would give more time for the Lyon's lawsuit to complete, and if the restraining order is removed it opens the possibility for lawsuits against Sony BMG across the country.

POLICY GUIDELINES

JUSTIFICATION

Guidelines need to be set so that users of music CDs have a reasonable expectation of privacy and safety on their computers. There must also be changes to the current policy to stop companies from preventing users from exercising rights granted to them in US Copyright Law, such as the first sale and fair use clauses.

INFLUENTIAL LEGISLATION

BALANCE ACT OF 2005

BALANCE stands for Benefit Authors without Limiting Advancement or Net Consumer Expectations. This truly describes what this bill seeks to accomplish: reach a compromise between copyright holders and consumers, such that consumers are able to use copyrighted material according for "fair uses" and the rights of the copyright holders are not infringed. The Digital Millennium Copyright Act all but removed the fair use doctrine from law in situations where some sort of copyright protection exists. Users are no longer allowed to circumvent this technology even for legitimate purposes such as creating a personal backup copy or ripping tracks onto a computer for personal listening. Representative Zoe Loftgren seeks to restore these rights.

To restore fair use to devices or media with copy protection in place, this act lays out certain circumstances under which protection circumvention is allowed. For a user to circumvent copy protection legally, he must be doing one of two things: making an archival backup for personal use or converting the copyrighted work to a format that can be used by other digital devices for personal use. The latter provision allows circumventing copy protection to rip CD tracks to a computer, for example, provided that the ripped tracks are not retransmitted or used for public performance.

The second part of the fair use section of this legislation allows users or companies to make protection circumvention tools available under certain circumstances. This is arguably the most controversial part of this legislation, since these tools inherently allow users to circumvent copyright protection with no real valid

means of determining whether such circumvention constitutes copyright infringement. This legislation states that making tools available for copy protection circumvention is legal provided that the following three circumstances are met: use of such tool is necessary for fair use (according to the above section), the tool is "designed, produced, and marketed to make a non-infringing use", and means for fair use circumvention are not provided by the copyright owner. It is also important to note that if copyright holders provide a means for lawful circumvention, it must be free and straightforward to use.

Finally, the BALANCE Act allows users to sell a digital copy of copyrighted material provided that all original copies are destroyed. This provision is reasonable, but nearly impossible to enforce. It is extraordinarily easy for a user to sell ripped tracks to multiple users while still maintaining or selling the original media. Without this provision, it is easy for law enforcement to verify if a user has the proper licenses. For music, for example, checking all of the media the user has and examining transactions with iTunes, Napster, and the other online music stores will yield an accurate list of allowed tracks can be assembled. The only potential exception would be tracks that were backed up from CDs that were lost or destroyed.

Overall, the BALANCE Act remedies many of the criticisms of the DMCA received. Fair use has been an important part of copyright law since its inception (albeit not in statute until relatively recently) and must be maintained. The BALANCE Act restores fair use and ensures that the public has the means by which to exercise its rights. [1]

DIGITAL MEDIA CONSUMER RIGHTS ACT OF 2005

The Digital Media Consumer Rights Act (DMCRA) has many of the same goals the BALANCE Act does: to reestablish fair use and ensure that consumers' rights are protected. The bill sponsors cited the confusion and disruption caused by new forms of copy protection along with the following two reasons that this bill is necessary:

(1) The limited introduction into commerce of "copy-protected compact discs" has caused consumer confusion and placed increased, unwarranted burdens on retailers, consumer electronics manufacturers, and personal computer manufacturers responding to consumer complaints, conditions which will worsen as larger numbers of such discs are introduced into commerce.
(2) Recording companies introducing new forms of copy protection should have the freedom to innovate, but should also be responsible for providing adequate notice to consumers about restrictions on the playability and recordability of "copy-protected compact discs".
(3) The Federal Trade Commission should be empowered and directed to ensure the adequate labeling of prerecorded digital music disc products. [11]

Additionally, this act seeks to expand the fair use section of the DMCA, adding general scientific research and non-infringing use to the allowable reasons for protection circumvention.

The first part of this legislation does not concern the DMCA at all, but rather seeks to put the Federal Trade Commission (FTC) in charge of ensuring that compact discs are properly labeled. The act outlaws improper or misleading labels and the removal or modification of labels prior to sale. Essentially, any disc is considered mislabeled if it fails to indicate its compatibility with computers or normal CD players. Also, if a CD does not display minimum software requirements, restrictions on song downloading to the hard disk, or the return policy should the disc not perform as expected, it is considered mislabeled.

Finally, the act outlines two additions to the exception cases under the DMCA's section on copy-protection circumvention. The first is the addition of a broader definition of research than the original exception for encryption research only. Under the DMCRA, any research into "technological measures" shall not be a violation. The final addition is an exception for circumventing access control for non-infringing purposes. The bill sponsors cite a blind person circumventing access control to have the computer read an eBook aloud as an example of this. This act also allows the distribution of such software or hardware as long as there is not "direct infringement." [11]

POLICY RECOMMENDATION

OVERVIEW

To protect the rights of users, it is important to have guidelines regarding the labeling of copy protected media, restrictions on the End User License Agreement, and the inclusion of software on music compact discs. These guidelines will help other corporations avoid incidents like the Sony XCP incident.

CD PACKAGING

It is important for consumers to know what they are buying before they buy it. Retailers generally do not allow users to return CDs after they have been opened, so it is important for users to be aware of the requirements and restrictions before they sacrifice their right to return the media. For this reason, corporations should include the relevant information on the exterior packaging of the CD.

The following information should be included in a standard labeling scheme on the outside of all copy-protected CDs:

- List of included copy protection – This list should include any software protection that is in place so users are aware that software is to be installed for them to use this compact disc. The minimum system requirements for the software must be listed so the user knows whether their processor-based media player can operate the copy protection software. Full disclosure of exactly what the software does is required (this includes, but is not limited to, why and when it makes access to the Internet, what files formats it is capable of converting media into, and any form of monitoring it will be doing on the user's system).
- If software is included, list limitations enforced: A user must know any restrictions on their use of the media including, but not limited to the number of times the media can be "ripped" to a computer, the compatibility of the media with standard devices used to play compact discs (including personal computers). This information will alert the user to any potential problems they may experience and make an informed decision.

- A list of devices the product is guaranteed to work with: Since some forms of copy-protection software make CDs and the derivative digital content incompatible with various media players (both processor-based and CDDA) the distributor must provide a list of device which the CD will work with. If the distributor chooses not to test various media players, a warning must be included: "This disc contains copy-protection software which may make its content unplayable on a variety of media players."
- Return policy: Due to potential incompatibilities with certain devices, there must be a return policy in place should the user be unable to use the media as indicated by the compatibility list. This will include recourse for a replacement disc should the original disc not operate in devices listed in the compatibility list. There must also be a warning to the user if the disc cannot be returned for a refund after the packaging is opened.

EULA RESTRICTIONS

While End User License Agreements (EULAs) have become commonplace in software, they are a relatively new phenomenon in compact discs. These agreements may impose certain restrictions on what the consumer is allowed to do with the enclosed content, but may not damage the rights granted to the user by copyright and merchandizing laws.

- The EULA must allow consumers to make an archival backup of any CD which they purchase as long they retain the rights of the original CD. The right to an archival backup is forfeited if the user chooses to exercise his right to resell the original CD. An archival backup is specifically defined as: An exact duplicate of the original CD including any copy protection software which was included. The manufacturer is not required to give a user the ability to make a copy of the CD free of copy protection.
- The EULA may not prevent the user from doing anything with the content which is protected by the Fair Use section of the Copyright Act of 1976. This includes the right to resell the CD. In "Softman Products Company, LLC, v. Adobe Systems Inc: Order re Application For Preliminary Injuction", United States District Judge Dean Pregerson stated, "the purchaser commonly obtains a single copy

of the software, with documentation, for a single price, which the purchaser pays at the time of the transaction, and which constitutes the entire payment for the "license." The license runs for an indefinite term without provisions for renewal. In light of these indicia, many courts and commentators conclude that a "shrinkwrap license" transaction is a sale of goods rather than a license." Since Pregerson deems any purchases involving an EULA as a sale, rather than a license, the EULA cannot prevent the user from reselling the CD under First Sale. [36]

- The EULA must contain provisions for the consumer to decline. Therefore, a policy and procedure for returning the CD must be specified in the EULA, and this procedure cannot put undue burden on the consumer. However, the return police can restrict the return procedure to a reasonable amount of time after the original purchase date. This reasonable time must be given so the user can fully read and understand the implications of the EULA and how it will affect their experience of the CD's content. Software manufacturers, such as Blizzard Entertainment and Microsoft, already have a clause in their software which states, or is similar to, the following: "If you do not agree to the terms of this agreement, promptly return the unused software program to the place of purchase, or contact Blizzard Customer Service at (800) 592-5499 for a full refund of the purchase price within 30 days of the original purchase." [2]
- The EULA may not force the user to waive Implied Warranty nor can it force the consumer to waive liability for damages caused by a manufacturing defect in the CD or the software included on the CD.

SOFTWARE

Copy protection software is within a corporation's scope of operation to protect their copyrighted material from piracy. However, consumers must have the ultimate ability to know and control what is installed on their computer at any time. Therefore, there are several restrictions which must be placed on the copy protection software. If the user chooses not to install the copy protection software on their computer, they must still be allowed to play the music in a different media player on their computer, though they may be restricted from making copies of the content.

- Before anything is installed on a consumer's computer, the user must be informed completely of what copy protection software is being installed and what the software will do. This includes warnings about the number of times music can be copied and to what digital formats the software permits the user to copy the music to.
- The copy protection software must be completely inert unless the user is making new copies of digital content onto their hard drive, a blank CD, or a portable device. The copy protection software cannot use any system resources on the consumer's computer unless one of these conditions is met. The copy protection software's files, processes, and registry entries must be visible to the user at all times. No form of cloaking technology can be installed to prevent the user, or anti-spyware/malware/virus software the user chooses to run, from looking at or scanning the installed copy protection software.
- If the copy protection software is designed with the ability to make internet connections for software or content updates, there must be an easily accessible option for the user to disable internet connections.
- At no time can the software, or internet connections made by the software, be used to collect personal information about the user.
- If at any time the user chooses to forfeit their ability to use digital content of a CD they own, they must be allowed to uninstall the copy protection software. An uninstall application must be included on the disk with the copy protection software, and must make a clean uninstall of all related files, processes, and registry entries. The uninstaller is allowed to leave files or registry entries which contain information about previous use of digital content, so that in the event the user reinstalls the copy protection software, they are still limited to the original number of copies set forth in the End User License Agreement.

BIBLIOGRAPHY

[1] "BALANCE Act of 2005". HR 4536. http://thomas.loc.gov/cgi-bin/query/z?c109:H.R.4536:.

[2] Blizzard Entertainment. "End User License Agreement", http://www.worldofwarcraft.com/legal/eula.html, 29 July 2004.

[3] "CD-ROM". Wikipedia. http://en.wikipedia.org/wiki/CD-ROM.

[4] "Compact Disc". Wikipedia. http://en.wikipedia.org/wiki/Compact_disc.

[5] "Copy Control". Wikipedia. http://en.wikipedia.org/wiki/Copy_Control.

[6] "Copyright Term Extension Act". Wikipedia. http://en.wikipedia.org/wiki/Sonny_Bono_Copyright_Term_Extension_Act.

[7] "Copyright Timeline". Association of Research Libraries, Washington, DC. http://www.arl.org/info/frn/copy/timeline.html.

[8] "Digital Millennium Copyright Act". HR 2281. http://thomas.loc.gov/cgi-bin/query/z?c105:H.R.2281.ENR:.

[9] "Digital Rights Management". Wikipedia. http://en.wikipedia.org/wiki/Digital_rights_management.

[10] Dix, Alan. "Moore's law - methods to study new environments". HCIBook.com. http://www.hcibook.com/e3/online/moores-law/.

[11] "DMCRA of 2005". HR 1201. http://thomas.loc.gov/cgi-bin/query/z?c109:H.R.1201:.

[12] Doctorow, Cory. "Sony Anti-Customer Technology Roundup and time-line", http://www.boingboing.net/2005/11/14/sony_anticustomer_te.html, 14 November 2005.

[13] "Economies by broadband penetration (2004)". International Telecommunications Union. http://www.itu.int/ITU-D/ict/statistics/at_glance/top20_broad_2004.html.

[14] Edelman, Ben. "Cleaning up Sony's Rootkit Mess", http://www.benedelman.org/news/112105-1.html, 21 November 2005.

[15] "Eldred v. Ashcroft". Wikipedia. http://en.wikipedia.org/wiki/Eldred_v._Ashcroft.

[16] "Fair Use". Wikipedia. http://en.wikipedia.org/wiki/Fair_use.

[17] "Fair Use". Stanford Copyright & Fair Use. http://fairuse.stanford.edu/Copyright_and_Fair_Use_Overview/chapter9/index.html.

[18] Felten, Ed. "Sony BMG and First4Internet Release Mysterious Software Update", http://www.freedom-to-tinker.com/?p=921, 3 November 2005.

[19] Felten, Ed and J. Alex Halderman. "Sony's Web-Based Uninstaller Opens a Big Security Hole", http://www.freedom-to-tinker.com/?p=927, 15 November 2005.

[20] Garrity, Brian. "Artists Take Stand Against Copy Protection". HollywoodReporter.com. http://www.hollywoodreporter.com/thr/music/article_display.jsp?vnu_content_id=1001221682.

[21] Graham, Jefferson. "Sony to pull controversial CDs, offer swap", http://www.usatoday.com/tech/news/computersecurity/2005-11-14-sony-cds_x.htm?csp=34, 14 November 2005.

[22] Hesseldahl, Arik. "Spitzer Gets on Sony BMG's Case", http://businessweek.com/technology/content/nov2005/tc20051128_573560.htm, 29 November 2005.

[23] "Home Computers and Internet Use in the United States: August 2000". Census.gov. http://www.census.gov/prod/2001pubs/p23-207.pdf.

[24] "Internet indicators: Hosts, Users and Number of PCs". International Telecommunications Union. http://www.itu.int/ITU-D/ict/statistics/at_glance/Internet04.pdf.

[25] Kamber, Scott. "In re SONY BMG CD Technologies Litigation Settlement Agreement", 28 December 2005.

[26] Kaminsky, Dan. "Welcome to Planet Sony", http://www.doxpara.com/?q=sony, 15 November 2005.

[27] "Lexmark International, Inc. v Static Control Components, Inc.". Electronic Frontier Foundation. http://www.eff.org/legal/cases/Lexmark_v_Static_Control/20030108_lexmark_v_static_control_components.pdf.

[28] Lieb, Rebecca. "Most Americans Have PCs and Web Access". Clickz.com. http://www.clickz.com/stats/sectors/geographics/article.php/3559991.

[29] Lyon, Mark. "The Sony BMG Settlement for XCP and MediaMax", http://www.sonysuit.com/, 6 February 2006.

[30] Michaelson, James. "James Michaelson and Ori Edelstein v. Sony BMG Music, Inc. and First 4 Internet", 14 November 2005.

[31] "MP3 Encoding". http://ntrg.cs.tcd.ie/undergrad/4ba2.01/group10/mp3.html

[32] Nikki, Matti. "Sony's XCP DRM", http://hack.fi/~muzzy/sony-drm/, 6 December 2005.

[33] Oberholzer, Felix and Strumpf, Koleman. "The Effect of File Sharing on Record Sales". http://www.unc.edu/~cigar/papers/FileSharing_March2004.pdf. (under revision)

[34] Office of the Attorney General. "Attorney General Abbott Brings First Enforcement Action In Nation Against Sony Bmg For Spyware Violations", http://www.oag.state.tx.us/oagNews/release.php?id=1266, 21 November 2005.

[35] One Stop CD Shop, LLC. "History of CD Technology". http://www.oneoffcd.com/info/historycd.cfm.

[36] Pregerson, Dean. "Softman Products Company, LLC, v. Adobe Systems Inc: Order re Application For Preliminary Injuction", 27 August 2001.

[37] "Red Book (audio CD standard)". Wikipedia. http://en.wikipedia.org/wiki/Red_Book_(audio_CD_standard).

[38] Reuters. "Sony Tests Technology to Limit CD Burning", http://news.cnet.co.uk/digitalmusic/0,39029666,39189658,00.htm, 1 June 2005.

[39] "RIAA Lauds State Criminal Action Against A Peer-To-Peer Hub Operator". RIAA.com. http://www.riaa.com/news/newsletter/082605.asp.

[40] Rich, Lloyd L.. "Indivisibility and Divisibility of Copyright: Copyright Act of 1909 and 1976". http://www.publaw.com/1976.html.

[41] Russinovich, Mark. "Sony, Rootkits and Digital Rights Management Gone too Far", http://www.sysinternals.com/blog/2005/10/sony-rootkits-and-digital-rights.html, 31 October 2005.

[42] Sandefur, Timothy and Post, David. "MGM Studios v. Grokster". Findlaw.com. http://news.findlaw.com/hdocs/docs/mpaa/acu030105brf.pdf.

[43] Schultz, Evan P.. "A Hidden Hope for Fair Use". Law.com. http://www.law.com/jsp/article.jsp?id=1052440872261.

[44] Sony BMG. "End User License Agreement". www.sysinternals.com/blog/**sony-eula**.htm, 7 January 2005.

[45] "Sony Corp. v. Universal City Studios, Inc.". Findlaw.com. http://caselaw.lp.findlaw.com/scripts/getcase.pl?court=us&vol=464&invol=417.

[46] Thurrott, Paul. "OS Market Share: Microsoft Stomps the Competition". WindowsITPro.com. http://www.windowsitpro.com/articles/index.cfm?articleid=40481.

[47] Ulaby, Neda. "Sony Music CDs Under Fire from Privacy Advocates", http://www.npr.org/templates/story/story.php?storyId=4989260, 4 November 2005.

[48] "United States Copyright Act of 1976". Wikipedia. http://en.wikipedia.org/wiki/Copyright_Act_of_1976.

[49] United States District Court for the Southern District of New York. "In re Sony BMD Technologies Litigation Hearing Order", 6 January 2006.

[50] "U.S. Manufacturers' Unit Shipments and Value Chart". RIAA.com. http://www.riaa.com/news/newsletter/pdf/2004yearEndStats.pdf.

[51] "US Copyright Law". Copyright.gov. http://www.copyright.gov/title17/circ92.pdf.

[52] "US Copyright Law". Wikibooks. http://en.wikibooks.org/wiki/US_Copyright_Law.

[53] Verrilli, Donald B. et al.. "Brief For Motion Picture Studio and Record Dist. Petitioners". http://www.eff.org/IP/P2P/MGM_v_Grokster/MGM_reply_brief.pdf.

[54] "Viruses use Sony anti-piracy CDs". BBC News. http://news.bbc.co.uk/1/hi/technology/4427606.stm, 11 November 2005.