Project Number: BYK - DRM1

Digital Rights Management: A Warning for the Future

An Interactive Qualifying Project

submitted to the Faculty of

WORCESTER POLYTECHNIC INSTITUTE

in partial fulfillment of the requirements for the

Degree of Bachelor of Science

Submitted by:

Vivek Varshney

Vivek Varshney

Date: January 10, 2007

Submitted to:

Professor Brian King, Project Advisor

Abstract

Digital Rights Management is a general term given to technology which serves to restrict access to content. This paper explains what Digital Rights Management is and what its purpose is. Prior art containing DRM policies will be analyzed to show why the reader should be aware of DRM, how DRM has been accepted by the market, and its potential ramifications. The paper concludes with suggestions about the future of DRM policies.

Acknowledgments

The author would like to thank Professor Brian King, WPI ECE, for his help and guidance during this project. Without his patience, this paper would not be possible.

Contents

List of Figures

Executive Summary

Information has flowed freely from among people. As soon as a practical method to store audio and video information was invented, people started to try to duplicate audio and video information. While technological advances made audio and video recordings easier to make and more practical to play, pirates, people who make use of or reproduce the work of another without authorization, had to deal with issues that hindered piracy, such as a physical distribution network, inherent in analog recording, and cost.

In the last 25 years, significant technological advances have made it far easier to copy media and distribute it. First, the use of digital media instead of analog allowed for 'bit-perfect' copies, or copies identical to the original, to be made. Next, advances in home computing power gave the average person enough computing power to perform audio and video compression in realtime. Additionally, advances in data storage technology for home and mobile applications made storing several hundred or thousand media files practical. Lastly, the advent of broadband Internet connections and peer-to-peer software allowed anyone to trade media with ease.

As content producers realized the relative ease with which content could be pirated, restrictions started to emerge to counter common methods of piracy. Digital Rights Management (DRM) is the general name given to any policy which determines how content can be accessed, copied, and distributed. DRM is a series of electronic locks for digital data (music, video, data). A lock and key can be thought of as an accurate analogy for DRM. DRM is the lock protecting what is behind the door, and those who possess a key can access the content.

This paper addresses the following questions regarding DRM:

1. What is DRM?
2. Why has DRM become prevalent, and what is its purpose?
3. What is the corporate view on the purpose of DRM?
4. What is the effect of DRM on society and the end user experience?
5. What effect does DRM have on piracy, and is it a viable anti-piracy measure for future content distribution?
6. How has the market reacted to the introduction of DRM enabled devices?
7. Is there a successful business model for distributing copywritten material where
   - Artists are fairly compensated?
   - Users have the freedom to do as they wish with purchased material?

Digital Rights Management started as a means for content producers, owners, and distributors to protect their Intellectual Property (IP). According to Microsoft Corporation, DRM is

> Any technology used to protect the interests of owners of content and services (such as copyright owners). Typically, authorized recipients or users must acquire a license in order to consume the protected material - files, music, movies - according to the rights or business rules set by the content owner [12].

DRM is more of a policy choice than a technology, where the policy being set is rules governing the use of the content. These rules are set by the owner, distributor, or whoever is in charge. Additionally, DRM can be changed at any moment, assuming the device is able to communicate with the central server. If the device is able to connect to a central server, the policy could change at any moment for any reason.

Media corporations have identified piracy as a problem and have determined DRM is a solution to that problem. DRM enabled products are used to help the Recording Industry Association of America (RIAA) reduce an estimated $4.2 Billion dollar loss of revenue to piracy each year [47], as well as enforce access controls set forth by the RIAA, the Motion Picture Association of America (MPAA), software companies, and anyone else who produces and distributes content.

Currently there are many consumer electronics which have some type of DRM built-in. For example, Digital Television (DTV) has the broadcast flag, or data which specifies the devices which can display content and states rules on recording the digital television stream. Other examples are any music or video product purchased from Apple's iTunes Store, Digital Versatile Discs (DVDs), software activation, and Trusted Computing (TC).

The restrictions in DRM can have an effect on the end user experience, as well as have social and ethical consequences. While DRM reduces piracy, it can also reduce legitimate access to content. DRM restrictions can potentially be changed at will by corporations, and abuse, such as surreptitiously changing content access rules, may be difficult to control as there is no group which monitors DRM rules. Additionally, the impact of license restrictions and laws passed relating to DRM make it difficult to pirate content and to use content legitimately, leading to various responses from consumers and consumer advocacy groups. In addition, two famous psychological experiments are mentioned to help aid in understanding the potential social and ethical ramifications of harsh policies and changing rules.

From the response to current DRM enabled technologies, DRM may not seem an appropriate response to reduce piracy. Additionally, consumer advocacy groups, such as the Electronic Frontier Foundation, argue that DRM actually increases piracy as consumers want access to content without restrictions and are willing to challenge laws passed in favor of DRM. Additionally, several DRM-enabled consumer products whose restrictions have been defeated are described in detail, such as the breaking of the Content Scrambling System (CSS) on DVDs, defeating software activation, and workarounds to remove Apple's Fairplay DRM from iTunes Store purchases.

Several business models exists with DRM, and their success is varied. The fifth chapter explains in detail the success of models such as the iTunes Store and Video on Demand. In addition, the explanations give lessons learned regarding DRM enabled content.

This paper then summarizes the findings and tries to determine if current content distribution methods are fair. Using the lessons learned from prior DRM enabled products and consumer sentiment, a determination is made as to whether DRM will doomed to failure.

The paper concludes with one possible view of DRM in the year 2050, as well as a future

method for content distribution. The future content distribution method will be controlled by the artists, consumers, and content distributors, with a series of checks and balances to ensure one group does not have too much power. Content would be purchased using an Internet store and distributed with a protocol similar to the BitTorrent protocol.

Chapter 1

Introduction

Since the invention of the printing press information flowed freely from person to person. Such was the case for hundreds of years, as information in various forms, such as books, diagrams, and paintings passed from people to people. People were free to make copies of information as long as they had the physical tools required and desire to produce a copy.

As soon as a practical method to store audio and video information was invented, people started to duplicate the content. Initially, audio and video duplication was difficult, as costly special equipment was needed to work the physical media for audio and to copy the film for video.

In the last one hundred years, significant technological advances in recording made recording and copying more popular. For example, 8-track media was a significant technological leap from the phonograph, allowing music to be more portable, as well as easier to produce and, thus it became popular. Further improvements in technology came with the introduction of the cassette tape, causing 8-track to lose in popularity. Examples of improvements in video technology are the Video Home System (VHS) and Betamax tapes, which succeeded reel to reel video. When VHS and cassette tapes started becoming popular, low cost equipment that could play the media became popular, and many of those players came equipped with recording mechanisms.

With the advent of cheaper and more easily available analog recording equipment, it was fairly straight-forward to make a copy. Thus, bootlegging of audio and video started to occur. Bootlegging, also known as illegally copying or pirating, provided an alternative method of obtaining material. While bootlegged media often sold for significantly less than official versions, the quality degradation in analog recordings helped serve to limit piracy.

The quality of analog recordings deteriorates with each subsequent copy. An original can be copied, but each subsequent copy was only able to be copied a finite number of times before the quality became poor. The noticeable deterioration in the quality of bootlegged material was part of the incentive to purchase the original.

Another issue that helped limit the amount of piracy was the requirement of a physical distribution network. After the problems in producing bootlegs of analog media were reduced, the next problem was to find an adequate distribution network. Since the bootleg was a physical object, it needed a physical distribution network, such as distributors, vendors, and buyers. The inherent problems in a physical network, such as analog duplication problems, having a distribution network and buyers, and evading authorities, caused an analog piracy network to require significant resources and kept piracy low. With the advent of digital media, most of these problems went away, as discussed next.

In the 1980s and 1990s digital storage methods were introduced and quickly became more popular than the existing analog technologies. The Compact Disc (CD) was introduced in 1982 for audio and the Digital Versatile Disc (DVD) was introduced in 1996 for video replaced their analog counterparts. The move to digital media meant if someone had equipment which could read the encoded data, they could theoretically make a perfect copy of the disc. When the CD was introduced, there was no practical method of copying music CDs. It was feasible to copy if one purchased CD recorders, not the kind found in computers, but the kind used to press aluminum CDs. This machine would allow making 'bit-perfect' copies, or copies digitally indistinguishable from the original. The ability to do 'bit-perfect' copies means copies were no longer susceptible to quality loss found in analog media.

The powerful corporations which sold content on the digital media realized 'bit-perfect' copies could be made, and saw bootlegs with 'bit-perfect' copies as a potential business threat. Thus the basic forms of copy protection were introduced. These primitive forms of copy protection were good first measures, but were often very easily defeated by bootleggers. While the quality barrier was eliminated with digital media, additional barriers to piracy included the excessive cost of purchasing copying machines, which was on the order of a million dollars, and the need to have a physical distribution network. The situation was similar for DVDs, released in the US in May 1997, even though DVDs were introduced almost 15 years later than the CD.

Intel Corporation's release of the Pentium Processor in 1993 made available an unprecedented amount of computing power to home users. This processor, and subsequent releases, were powerful enough to perform file compression for audio files in real-time. Since desktop computers were also shipping with CD drives, and eventually DVD drives, nearly any home user could insert a CD into their computer and copy it, assuming they had the necessary software. These compressed formats made the file size an order of magnitude smaller while retaining a level of sound quality that nearly all people found acceptable.

At the same time as high performance computers were becoming available to the average consumer, storage devices were also making improvements. Without a sufficiently large storage device, it was impractical for people to store uncompressed content on a computer, as there was just not enough space for the media and the necessary files required to run the computer. Recordable media, such as CD-R/RWs became more popular, allowing consumers to copy content to CDs. The CD-R/RWs eventually gave way to DVD-R/RWs, which allowed significantly more content to be stored. With DVD-R/RWs, consumers could store more than a dozen ripped albums on a single disc. Additionally, hard drive manufacturers were making significant leaps in technology, allowing the consumer to have unprecedented amounts of storage space in their home computer. All of this additional storage space made it more practical to store the large of amount of data in media on a computer, thus lowering the barrier to piracy.

At the same time storage was improving for the home computer, storage technology for mobile devices was also improving. Flash memory, a type of memory commonly found among portable devices, was increasing in density, or the amount of data per unit area, and decreasing in size with each generation. While flash and other mobile capacity was not as large as storage technology found on the desktop, it was large enough that several hundred compressed audio files or a few video files could easily be stored. This opened up a market for portable media devices, devices which were capable of storing media and portable enough to be carried by a person.

Around the same time as storage technology was improving, Internet connections improved significantly as bandwidth increased and access to broadband connections increased. Internet users were used to using dial-up connections, which used low bandwidth phone lines, and were not very fast at transferring large files. Communications companies began rolling out higher bandwidth connections, such as Digital Subscriber Lines (DSL) and cable modems. These connections were significantly faster than their predecessor, phone modems; as a consequence, sending large files took less time. People began to utilize high bandwidth connections to distribute media and realized this type of network made it possible to distribute content with an unprecedented amount of ease.

Programs such as Napster allowed anyone with an Internet connection to download music from anyone who shared music and was part of the Napster network. With broadband Internet connections, the hurdle of a physical distribution network was eliminated. Since the content was digital, and high speed connections were becoming very common, the barrier to piracy was significantly lower and the average consumer could quite easily become involved in bootlegging music and video. People seemed to participate with very little concern over the legality of their act.

Programs such as Napster, which allowed for easy content distribution over what is called peer-to-peer networks (p2p) caught the attention of the Recording Industry Association of America (RIAA) and Motion Picture Association of America (MPAA). These two organizations became infuriated at the level of piracy which software such as Napster allowed. During the start of p2p networks, there was no way to stop people from distributing copyrighted material and also no way to catch and punish those who did. The RIAA and MPAA started to file lawsuits against some of the more common users of programs such as Napster in an attempt to reduce the amount of piracy. In addition, they, as well as other corporations, started to determine the next generation of copy protection schemes.

With the barriers to piracy significantly reduced, media companies decided it was time to update their copy protection methods. The next generation of copy protection is called Digital Rights Management (DRM). According to IBM Corporation,

> The goal of DRM technology is to simply limit compatibility because things that are compatible can be copied and distributed freely. The majority of DRM technology is aimed at ensuring that people pay for products they might otherwise just make copies of [56].

This view of DRM may or may not be accurate, as we will explore later on. In general, DRM is

> The umbrella term given to any electronic technology which enforces policies pertaining to access of software, music, movies, data, and other digital and analog content. In more technical terms, DRM handles the description, layering, analysis, valuation, trading and monitoring of the rights held over a digital work. In the widest possible sense, the term refers to any such management [66].

DRM can be thought of as a set of electronic locks for digital data (music, video, data). It is a wrapper around the raw data [6]. For example, DRM is the lock, and the lock is protecting what is behind the door, in this case, digital data. The only people who can legally access the content are those who possess "keys" which open the lock. One can possess a key in various ways, and methods of possession can be legal or illegal, such as purchasing a key from the distributor of the content or breaking the lock.

This paper discusses what DRM is, how it has come about, the positive and negative aspects of DRM, and why the reader should be concerned about DRM. This paper will try to address the following questions with regards to DRM:

1. What is DRM?

2. What is the purpose of DRM?

3. Why are large corporations in favor of DRM?

4. What effect does DRM have on the end user experience?

5. How has the market reacted to technology with DRM included?

The next section will discuss what DRM is and how is has evolved. After that, the purpose of DRM and the effects of DRM will be reviewed, as well as whether DRM is solving the problem it was introduced to solve. After that, an analysis of products containing DRM will be presented and the market response to them. Next a discussion of current business models using DRM will be presented. Lastly, the future of DRM will be presented given the current trends.

Chapter 2

Background

This section will present a detailed background on Digital Rights Management (DRM). During the detailed background, a complete definition of DRM will also be given. Additionally, reasons for media producers introducing DRM will be presented, as well as the goal of DRM. This section will also explain why DRM is a policy choice set by the content distributors and not a particular implementation of technology.

2.1 What is Digital Rights Management?

Chapter 1 gives a very brief history of information copying. From Chapter 1 we learned the most general definition of DRM is any technology which enforces a policy that limits reproduction of digital data. DRM can be contained in any media but has mostly been found in copyrighted material such as, but not limited to, electronic books (eBooks), music (CDs and most downloadable music), software, movies (DVDs), downloadable television shows, and digital television broadcasts. For a DRM policy to work, it must be played through an electronic device which supports the desired policies.

Any copyrighted material can be encapsulated in some form of DRM as long as it is digital in the first place. This means content such as eBooks, CDs, digital music, DVDs, and software can be wrapped in some form of DRM.

According to Microsoft Corporation, DRM is defined as

> Any technology used to protect the interests of owners of content and services (such as copyright owners). Typically, authorized recipients or users must acquire a license in order to consume the protected material - files, music, movies - according to the rights or business rules set by the content owner [12].

It is important to note that DRM and copy protection are not synonymous. Copy protection is technology which prevents duplication of media, and copy protection methods have improved over time as each implementation usually improves holes which were discovered in previous implementations. It is important to note that a particular implementation of copy protection is static. Copy protection is a subset of DRM. DRM is a set of rules which govern how content can be used. While a particular rule of DRM could be enforced by copy protection technologies, other rules such as limits on what and how many devices which are allowed to use content, and who is allowed to use content, are enforced by other technologies.

This makes DRM more of a policy choice than technology, and the policy being the set of rules governing the use of the content set forth by the owner, distributor, or whoever is in charge. Additionally, DRM has been designed so it can be changed at any moment, assuming the device is able to communicate with the central server. If the device is able to connect to a central server, the policy could be changed at anytime for any reason, whether it be to loosen or tighten the rules governing the use of content.

An example of a DRM policy would be the DiVX technology that was introduced by Circuit City in the late 1990s. The DiVX discs initially were available for a pay-as-you-play model, but when Circuit City realized their scheme was a unsuccessful, they reprogrammed the restrictions to be open and removed any DRM locks.

During the early part of this decade (early 2000s) DRM schemes became widely adopted in artistic works, such as music and movies. For this reason DRM has some association to music and movies, but it is important to note that DRM is not limited to just these products. DRM is found in software, such as Microsoft Windows XP, Microsoft Office, Turbo-Tax, and Adobe Photoshop. In Windows XP there is a tool which runs during installation to verify the serial key used to install Windows is legitimate. This program can cause Windows to refuse logins after a set period of time if illegal serial keys are used. Microsoft Office also has a similar feature, where the product must be "activated" within a set period of time; this activation checks the serial key used during install to verify authenticity.

2.2 Why has Digital Rights Management started?

Now that we understand what DRM is, the next topic to explore is why content producers and distributors feel a need to include DRM. To start, the modern entertainment industry was born around the turn of the 20th century. The gramophone was a new technology that allowed playing music in the home, and silent movies were starting to become more popular in theaters. Until the early 1980s music was distributed in analog forms, and until the mid to late 1990s movies were also distributed in analog forms [6].

The Recording Industry Association of America (RIAA) is an association that consists of all the major music label companies. Of them, there are four which are referred to as the Big Four - Sony-BMG, Time Warner, Universal, and EMI as they make up almost 80% of the market. Most artists will end up signing with one of these major labels. The RIAA also ends up controlling the price of music CDs, as well as the amount record labels pay their artists.

The impact of computers on the music industry has been very important for the last twenty years. The main issues of concern to the RIAA are that with computers, it is very easy to make a perfect copy of a CD, as well as compress the music, or encode that music, in a much smaller format (MP3, Ogg, *etc*) that allows for easy transmission over the Internet. The Motion Picture Association of America (MPAA) has an almost identical concern as the RIAA, differing only in that video is distributed instead of audio, as similar tools allow DVDs to be copied easily onto other DVDs or compressed and distributed fairly easily on the Internet. Since the prevalence of high speed, highly powerful computers, encoding music or movies has become trivial. In addition, the advent of broadband connections has made it easier for one person to upload a song or movie and allow many (tens, hundreds, thousands) people to download a copy. The RIAA and MPAA see this as theft of their Intellectual Property (IP), which they call piracy.

When using analog media, such as cassette tapes, it was still possible to duplicate a cassette and distribute it to a few friends. The problem with analog copies was that each copy had a slight but noticeable loss in quality, meaning after only a few copies it became quite difficult to try and continue distributing copies as copies fell below a desired quality level. Digital forms of media allow for perfect copies, meaning there is no loss in quality if copied one time, one thousand times, or even one million times. Additionally, a distribution network was usually very small, limited by the fact that a physical copy had to be passed from person to person. With 49.5 million people in the United States connecting to the Internet with a broadband connection in 2004 [42], digital copies have the potential to be distributed to a significantly higher amount of people than before.

Napster was a program that was very popular for pirating music in the early part of this decade. Using Napster, a user connected to a central server was able to search for songs shared by many (hundreds to thousands) of similar users. The program also facilitated the downloading of songs. In its peak, Napster had approximately 50 million users and had peak downloads of 2.8 billion songs in a month [6].

Since Napster shut down, other services came to replace it. Some of the new alternatives were similar to Napster, while others varied greatly, such as BitTorrent, Apple's iTunes Store, a new legal generation of Napster, and AllofMP3.com. It is important to note that some of these services are authorized by the RIAA, such as the new Napster and Apple's iTunes Store, while others are widely considered illegal such as downloading via BitTorrent and AllofMP3.com [17].

The problem with downloading music or movies with software such as Napster is that it is illegal under the current United States copyright laws. The law implies the music must be purchased legally, allowing the artists to be compensated, but Napster did not have a means to make purchases legal. US copyright laws do not allow it, nor do the owners of the IP, the RIAA/MPAA, and they consider this piracy. The response to the relative ease with which content could be copied gradually led to more and more sophisticated techniques to prevent copying and distributing content. These techniques are what is presently considered DRM. It is quite feasible that DRM conceived to help alleviate the piracy problem, although they do not seem to be limiting themselves to just that method.

Protecting IP is not something that was developed within the last century. The purpose of the US Patent and Trademark Office (USPTO), which has existed since its creation in the late 1700s, is to help people protect their IP with patents and trademarks. The USPTO defines a patent as

> A property right granted by the Government of the United States of America to an inventor to exclude others from making, using, offering for sale, or selling the invention throughout the United States or importing the invention into the United States for a limited time in exchange for public disclosure of the invention when the patent is granted [49].

Thus we can see patents are intended to protect the IP of the inventor and to encourage development of new inventions by rewarding the initial inventor. Predating the USPTO, one can find evidence that the colonial governments in the Americas (1600s) issued patents for inventions as far back as 1641 [39].

The RIAA has identified piracy as a huge problem. Directly on their website is a list of categories for piracy:

- Pirate recordings are the unauthorized duplication of only the sound of legitimate recordings, as opposed to all the packaging, i.e. the original art, label, title, sequencing, combination of titles etc. This includes mixed tapes and compilation CDs featuring one or more artists.

- Counterfeit recordings are unauthorized recordings of the prerecorded sound as well as the unauthorized duplication of original artwork, label, trademark and packaging.

- Bootleg recordings (or underground recordings) are the unauthorized recordings of live concerts, or musical broadcasts on radio or television.

- Online piracy is the unauthorized uploading of a copyrighted sound recording and making it available to the public, or downloading a sound recording from an Internet site, even if the recording isn't resold. Online piracy may now also include certain uses of "streaming" technologies from the Internet[47].

The RIAA also publicly states part of their response to piracy on their website. The RIAA says

> The RIAA-assisted raids have closed down hundreds of U.S. and overseas manufacturing and distributing operations, and significantly reduced illegal CD and cassette vending around the country [47].

Their response is not just limited to physical locations, but also involves a team on the Internet. Their website says

> In cyberspace, the RIAA's team of Internet Specialists, with the assistance of a 24-hour automated web-crawler, helps to stop Internet sites that make illegal recordings available [47].

Also, they say

> Based on the Digital Millennium Copyright Act's (DMCA) expedited subpoena provision, the RIAA sends out information subpoenas as part of an effort to track and shut down repeat offenders and to deter to [sic] those hiding behind the perceived anonymity of the Internet.[47]

While the RIAA website mentions what they are doing to combat piracy, there is no direct mention of DRM at all. However, an example of their use of DRM is found in any song purchased legally from an online music store. The downloaded files always have some sort of restrictions which limit the number of computers they can be played on, which programs can be used to play them, as well as which portable devices, if any, are capable of playback.

Perhaps the RIAA's most compelling reason to fight piracy is due to the estimated revenue loss. Regarding lost revenue, their website says

> Each year, the industry loses about $4.2 Dollars billion to piracy worldwide. We estimate we lose millions of dollars a day to all forms of piracy [47].

Losing a few billion dollars a year is a significant amount that will not be ignored by any corporation. A search of the RIAA website does not say how they reached that number; for now let us assume they in fact have some valid way of calculating this value [47].

Chapter 3

Examples of Digital Rights Management

This section will explore some common household products which contain some form of DRM. These products may be in your own home and used by you, or could be potentially relevant to you in the near future. These common products, which may initially appear free of DRM, may in fact have DRM silently included but not presently enabled. Examples of such include televisions, DVD players, computer software, and digital video recorders.

3.1 Broadcast Flag

To start, let us examine the format for the upcoming Digital Television (DTV) proposed by the Federal Communications Commission (FCC). When the switch to DTV occurs in 2009, it will affect nearly ever household in the United States. While it may not always be apparent, there is more than just audio and video data in a DTV broadcast. One feature of DTV is the Broadcast Flag, which is a series of status bits that specify restrictions and preservation of recording the content [19]. The extra data delivers policies which govern the use of the content as set by the creator and distributor of the broadcast. This flag enforces a policy which restricts saving content on disk drives, decides if recorded content should be of lower quality than the original, determines the inability to skip commercials, or even the ability to prevent content recording. In the United States, new television receivers and capture cards were supposed to incorporate this standard by July 1, 2005, but a federal court overturned this ruling. According to the Electronic Frontier Foundation (EFF), a US based non-profit with the purpose of preserving free speech rights in the digital age, the FCC had lacked the authority to force DRM into digital television tuners:

> Originally, an FCC ruling made it illegal as of July 2005 to manufacture or import DTV tuners unless they included DRM technologies mandated by the FCC. EFF and a coalition of libraries and public interest groups then sued to overturn the ruling. In a unanimous decision, the DC Circuit Court of Appeals concluded, as we had argued, that the FCC lacked authority to regulate what happens inside your TV or computer once it has received a broadcast signal [22].

Due to the work of the EFF, this technology is presently not mandatory on all TV capture cards. However it should be noted that while this ruling does not mean all tuner cards MUST include the broadcast flag, it does not force manufacturers to produce cards that lack support for the broadcast flag, meaning a manufacturer does not have change an already existing design.

3.2 iTunes Store

Music has been very popular in the digital age. There are significantly more portable digital music players on the market than all forms of portable analog music players. While Apple Computer only started selling TV shows online in 2006, several companies, Apple included, have been successfully selling music online for several years.

Music is very popular with everybody. Kids and young adults, specifically college kids and teenagers, are big consumers of digital forms of music. One of the most popular music download services is the iTunes Store. Apple Computer Corporation's iTunes Store currently has over 70% of the PC-based digital music download market [43], and one can legally purchase and download music which contains restrictions in copying music. The iTunes software lets you use downloaded songs in as many playlists, lists of songs for playback, as you wish [8].

According to Apple's website, one can do the following with purchased content:

> Burn songs onto an unlimited number of CDs for your personal use, sync music to an unlimited number of iPods and play songs purchased from the iTunes Store on up to five Macs or Windows PCs [8].

Searching further on their website, we find what specifically they mean by only being able to play purchased music on up to five computers:

> Songs purchased on the iTunes Store can be copied to an unlimited number of computers. However, only five computers at a time can play your purchased music. You can enable a computer to play your purchased music by "authorizing" it. You can remove a computer from the authorization list by "de-authorizing" it. De-authorizing your computer does not erase your music files; it simply prevents your purchased music from playing until you authorize that computer again [9].

A few minutes spent on the popular search engine Google (www.google.com) for the string 'iTunes DRM' will show a series of pages regarding breaking the DRM in iTunes files.

The iTunes Store is an example of a product where the DRM policy is implemented entirely in software, meaning the restrictions could potentially change over time. However, if the DRM policy was implemented in hardware, especially hardware which is in the hands of many consumers, changes in policy would be difficult to make. The next example entails a system that enforces DRM in hardware.

3.3 DVDs: Content Scrambling System and Region Codes

The next technology containing DRM, Digital Versatile Discs (DVDs), can be found in most homes in the United States. The authors of the DVD standard incorporated two methods to help reduce piracy, the Region Coding scheme and the Content Scrambling System(CSS).

The idea behind region coding was to break up the world into eight regions as described below and seen in figure 3.1:

- 0: Informal term meaning "playable in all regions"
- 1: Bermuda, Canada, United States and U.S. territories
- 2: The Middle East, Western Europe, Central Europe, Egypt, Greenland, Japan, Lesotho, South Africa and Swaziland
- 3: Southeast Asia, Hong Kong, Macao, South Korea and Taiwan
- 4: Central America, the Caribbean, Mexico, Oceania, South America
- 5: The rest of Africa, Former Soviet Union, the Indian subcontinent, Mongolia, North Korea
- 6: Mainland China
- 7: Reserved for future use
- 8: International venues such as aircraft, cruise ships

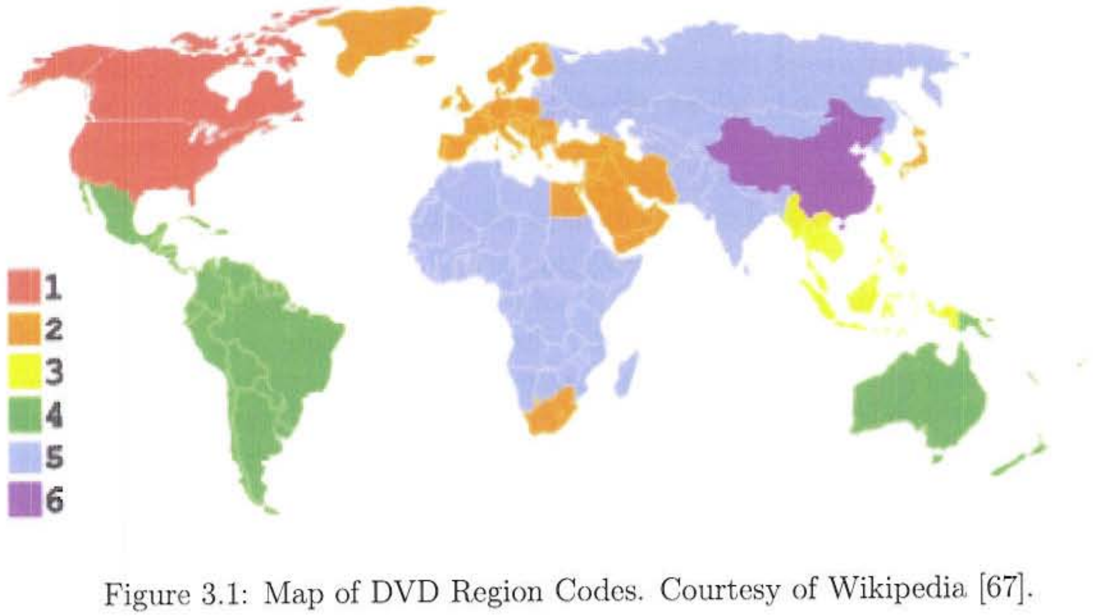

Figure 3.1: Map of DVD Region Codes. Courtesy of Wikipedia [67].

The idea behind the region coding scheme was to help reduce piracy by limiting the number of countries in which a DVD can be played. For example, a person living in the United States who purchases a region 2 DVD from a bootleg vendor can not play the disc (legally) at his house. However, this also has a drawback as a legally purchased DVD from another region can not be played outside its intended region, unless the disc was made region free. DVD players would see the disc marked as outside its allowed region and thus refuse to play it, rendering the content useless.

The next anti-piracy system incorporated is CSS. CSS uses 40-bit encryption to encode the DVD media in order to make it difficult to decrypt and rip (extract from the disc) as compared to non-encrypted DVD media. When the DVD format debuted, commercially available software DVD players were available on Windows and Macintosh computers and were being purchased. However, there were no DVD players for Linux-based computers which could play the encrypted DVDs. In an attempt to play DVDs on Linux, Jon Johansen, a teenager from Norway, attempted to break the CSS encryption. He successfully reverse engineered the format and released a program called DeCSS. DeCSS unscrambled the content and allowed one to view the data on a DVD without difficulty. Legally purchased DVD players have code similar to DeCSS which is obtained by licensing from the MPAA.

3.4 Activation in computer software

The next example of DRM pertains to computer software and is potentially important to anyone who uses or owns a personal computer. Current computers contain many different software programs from many different sources. A new trend in computer software is to include either a feature called product activation or install the software with all features but only allow use of certain features which a server authorizes. In the first case, during installation the software connects to the software maker's server on the Internet in order to verify its authenticity, then allow the user of the software to proceed as normal if the software is deemed to be legal, or shut out access if the copy is deemed to be illegal. For the second case, all the features of the software are installed, but each time the software is run it connects to a server and only allows use of features which are approved by the server.

According to Microsoft Corporation, the reason for including activation is:

- Why is Microsoft asking customers to activate their software?

  Microsoft designed Product Activation as a simple way to verify the software license and thwart the spread of software piracy. People who use illegal software not only hurt themselves, they also contribute to a problem that cumulatively can hurt job creation locally and regionally in the software industry and related businesses. Software piracy is an enormous drain on the global economy, according to the 2000 BSA Software Piracy Report. The report estimates worldwide losses in 2000 due to software piracy at almost $12 billion. Software piracy also has a significant impact on the high-tech industry, resulting in lost jobs, decreased innovation and higher costs to consumers.

- How will Microsoft Product Activation help thwart piracy?

Product Activation will help reduce casual copying by ensuring that the copy of the software product being installed is legal and has been installed on a PC in compliance with the End User License Agreement (EULA). Installations beyond those allowed in the license agreement will fail to activate.

- Haven't companies tried to implement anti-piracy technologies before and failed?

  Anti-piracy technologies that have been used in the past have not been easy for customers to use and were generally viewed as unacceptable by customers and the industry. For example, some early PC products required specialized hardware components or boot diskettes that were cumbersome for the user. Product Activation is a breakthrough technology in that it makes activation a natural part of setting up the software and avoids the pitfalls of anti-piracy methods used in the early days of the PC industry.

- How does the customer benefit from this approach?

  Over time, reduced piracy means that the software industry can invest more in product development, quality and support. This ensures better products and more innovation for customers. Ultimately, customers will benefit from the economic impact of reduced piracy through more jobs and higher wages. Customers will also receive the best value for their software investment by being able to receive product updates and other product information. Product Activation also helps prevent unsuspecting customers from purchasing counterfeit software. Customers who purchase counterfeit products could find they are missing key elements, such as user manuals, product keys, certificates of authenticity and even software code. They may also find that the counterfeit software contains viruses or does not work as well as the genuine product does [14].

From the above, it is clear that Microsoft Corporation's position on including product activation is to help reduce piracy. From other parts on the www.microsoft.com website, we see that a product has 30 days from install to be activated, otherwise the software will automatically expire (the program will refuse to load).

Another prominent software company, Macromedia, has the following to say about product activation:

- Is product activation the same as registration?

  No. They are two separate procedures. Product activation is an anonymous, secure, hassle-free process that verifies the legitimacy of your product serial number as well as deters the unlicensed use of Macromedia software. In contrast, product registration is a voluntary process that entitles you to product updates and special offers from Macromedia.

- What if I don't have an Internet connection?

  You have a 30-day trial period before you need to begin the activation of your software by entering in your serial number. If your computer is temporarily offline, you can still input your serial number and your software will run.

Activation will automatically complete the next time you are online and you launch your product. Once the product is activated, you do not need to be connected to the Internet to use the product.

- What information is collected and transmitted in the product activation process?

  We collect the minimum information required to successfully verify the product license for each product installation, which includes: the product serial number, product name, product version, and language; the operating system name, operating system version, and language; and your computer's processor and hard-disk type. This information is combined, encrypted, and then sent to Macromedia for verification. None of the collected information can be used to identify you or your individual hardware components in any way [10].

From Macromedia's website, we become aware that the software has to be connected to the Internet within 30 days of installation in order to complete the activation process. In addition, Macromedia only claims a few other pieces of information are sent to their servers, such as computer configuration.

From this section, we see major software companies claiming the use of activation software will reduce piracy. Software crackers on the Internet have produced "hacks" to remove activation within various pieces of software even though reverse engineering software to remove this sort of function is illegal.

3.5 Digital Millennium Copyright Act and copyright law

One law which essentially bans reverse engineering in software is the Digital Millennium Copyright Act (DMCA). It was passed in 1998 and criminalizes reverse engineering and distribution of any measures meant to circumvent copyright protection within the United States [65]. This means anyone who attempts to reverse engineer any of the DRM locks in the US is subject to prosecution in the US. This law has been used by many corporations in order to prevent distribution of DRM breaking or related breaking software, algorithms, or source code, such as the case with DeCSS. Originally, this bill was supported by the software and entertainment industries, but opposed by scientists, librarians, and those in academia for fear of being too restrictive [21]. An interesting note is that while this law only pertains to the United States, and does not apply to other countries, the role of copyright law internationally is a major topic which is very important and out of the scope of this paper.

3.6 Trusted Computing

Trusted Computing (TC) is a change in the way computer programs are run. The movement is backed by software and hardware companies, and its goal is to make computers more secure by using only approved hardware and software. This is done by forcing only approved software to run only on approved hardware as an attempt to reduce the possibility of malicious use. There are provisions for including secure access with authorization to use specific resources in the computer, allowing use if the program is deemed authorized and locking the program out if it is determined to be unauthorized. TC is backed by the Trusted Computing Group (TCG). They claim the purpose of TC is to improve computer security, reduce malware and viruses, and improve computers by only allowing authorized code to run.

> Trusted computing encompasses four key technology concepts, of which all are required for a fully trusted system.
>
> - Secure Input and Output
> - Memory curtaining / Protected execution
> - Sealed storage
> - Remote attestation [29]

Details on how exactly these key concepts work can be found on the Trusted Computing website, as well as in advanced computer science textbooks. Using the above methods seems to be an unusual way to improve security. It appears to take away control of the computer from the user/owner and place that in the hands of software makers, computer manufacturers, hardware makers, and others who are not the owners of the computers.

The EFF describes in great detail why TC is dangerous. Their arguments can be found in the publication "Trusted Computing: Promise and Risk", and are summarized below:

- Software interoperability and vendor lock-in: A server could force users to use only approved software if they wish to deal with a website or other server; unauthorized software could simply be ignored; this could force using only one vendor's software, then allowing the vendor to have a virtual monopoly.

- DRM, forced upgrades, forced downgrades, tethering: One thought for the move to TC is to allow software to have DRM. Another thought is that forced upgrades, which would be possible with TC, may insert new features such as DRM into software, and force users to obey certain policies. This could also tie a user's computer to a particular software or particular set of software for any given purpose, thus giving a vendor a virtual monopoly.

- Computer owner as adversary?: The current guidelines do allow for the execution of policies against the wishes of the computer owner and operator. This means the owner and operator lose control of their own machine [54].

3.7 Electronic Books

Electronic Books (eBooks) are digital forms of books and may contain DRM of some sort. With a digital copy of a book, it would be feasible to easily distribute the copy to almost anyone without ensuring the writer of the book receives proper compensation. In order to try and combat piracy, the authors of several eBook formats inserted some digital restrictions.

These restrictions include inability to copy the file, track readers and reading habits and send them to a publisher's server on the Internet, restricting how many times a document can be opened (or read), and restricting printing [68].

eBooks do not seem to have gained to much popularity as of 2006 for any number of reasons. Some users do not feel restrictions in the digital files are justified nor outweigh the benefits of having a digital copy. Some users feel a paper copy is more tangible, thus more valuable, and can not agree to paying the same amount for a digital copy. Other users do not want the hassle of having to use electronic devices in order to gain access to text they have purchased.

In 2005, worldwide ebook sales totaled roughly $12 million, compared to $31.6 billion in sales of books in the US. Ebook sales grew by 23% from 2004 to 2005, but their total sales is still barely a fraction of a percent compared to print books [20].

3.8 V-Chip

In the television sector, the V-Chip can be used to block content from being displayed. The V-Chip is an Integrated Circuit (IC) that implements rules released by the FCC on the ability to block the display of TV programming based on its rating. The Telecommunications Act of 1996 encouraged broadcasters to voluntarily establish a rating system [7]. Broadcast content is now rated, and these ratings can be seen in the top corner of the TV program, usually for a few moments when the program starts. Based on these ratings, the V-Chip, found in all TV sets manufactured after January 1, 2000, has the ability to prevent the display of content with certain ratings. This system is intended to prevent children from seeing content intended for mature viewers, such as violence, and sexually explicit content. The controls are usually set by the owner of the TV, usually assumed to be the parent of the child [7].

V-Chips in their current form appear to be a mild form of DRM. TV content is not blocked unless the function is activated by the owner of the TV. From this section, we see that there is another form of DRM present significant numbers in many houses.

Chapter 4

Methodology

The goal of my paper is to investigate, understand, and discuss many questions regarding DRM. The primary list of questions I will consider are:

1. What is DRM?
   The reader is presented with a complete definition of DRM in the first and second chapters of this paper. In addition, the third chapter presents some household products which contain DRM to emphasize how common DRM enabled products are.

2. Why has DRM come about, and what is its purpose?
   An overview of why DRM is in use is presented in the second chapter of this paper. Additionally, the second chapter also summarizes the purpose of DRM, with chapter five going into great detail on the purpose of DRM as described by media corporations, content distributions, consumers, and consumer advocacy groups.

3. What is the effect of DRM on society and the end user experience?
   The effect of DRM on society is presented in the fifth chapter. The effect of DRM on the end user experience is also presented in the fifth chapter. Additionally, psychology experiments will be presented to help fully understand the social and ethical behaviors of individuals and society.

4. What is the corporate view on the purpose of DRM?
   While chapter two gives an overview of what corporations view DRM as a solution for, chapter five explores in detail what corporations feel the purpose of DRM is. Additionally, what consumer advocacy groups say about DRM will be presented in order to keep a balanced viewpoint.

5. What effect does DRM have on piracy, and is it a viable anti-piracy measure for future content distribution?
   In order to explore whether DRM is successful in combatting piracy, it will be necessary to see if DRM has any effect on piracy. In order to answer this question, consumer reaction to piracy will be presented, as well as opinions on whether DRM is successfully combating piracy from corporations and consumer groups.

6. How has the market reacted to the introduction of DRM enabled devices?
   Chapter five will present how consumers have reacted to DRM enabled devices. In order to judge whether DRM is successful in combating piracy, it is crucial to understand why particular DRM enabled devices are successful or considered failures.

7. Is there a successful business model for distributing copy-written material where

   - Artists are fairly compensated?
   - Users have the freedom to do as they wish with purchased material?

   Several different content distribution models will be presented during this analysis. In order to judge if a model is fair for artists and if users have enough freedom, artist and consumer reaction will be presented, and a judgement on which is best will be made. Additionally, the author will present possible content distribution model for the future.

To answer these questions, the author will present an unbiased description of the facts. To be as accurate as possible, information gathering will be limited to only select, credible sources. Great care will be taken to ensure that any information obtained from the Internet (World Wide Web) is from credible sources, not any website. A source can be deemed credible if content is published by a well known professional society, such as the IEEE or by a reputable newspaper. Also if a credible source cites another source, that second source will be considered to be credible.

Information will be gathered in a variety of forms, including but not limited to reading articles from Internet news sites such as CNET, exploring corporation's websites for pertinent information, and reading newspapers such as the Washington Post and USA Today. Additionally, interviews with officials from corporations and school administration, such as Benjamin Thompson, Associate Vice President for Information Technology & Associate Chief Information Officer at Worcester Polytechnic Institute, will be conducted to obtain information first hand. Lastly, papers and opinions of lawyers and consumer advocacy groups will be presented in order to obtain a balanced viewpoint.

Along with presenting the information that has been collected, a detailed analysis will be conducted. In the analysis, key observations and comments on what has been found shall be made in order to fully understand the information. In addition, criticism, praise, and lessons learned will be given as appropriate. Lastly, the reader will be presented with the author's extrapolation of what may be the future of DRM.

Chapter 5

Discussion and Analysis

The purpose of this chapter is to find out what corporations feel about DRM in their digital products. Once the reasons are given, an analysis will be presented, specifically whether the consumer should trust what the corporations have to say. The social impact of DRM on individuals and the impact of DRM on society will be presented, aided by lessons learned from important psychological experiments. Additionally, more consumer products with DRM will be presented, along with the market response to these particular DRM enabled devices and the lessons learned. Lastly, business models with DRM will be explored.

5.1 What is the purpose of DRM?

This section will try to understand the purpose of DRM. First the views of the large corporations backing DRM will be presented, then an analysis of their reasoning will be presented. Additionally, the issue of trusting the corporations will be examined and solutions to existing concerns will be proposed.

5.1.1 What do corporations think about DRM?

For Apple, the inclusion of their 'Fairplay' DRM was done in order for the RIAA to allow Apple to sell music online. Fairplay is Apple's version of DRM, which they claim is fair for the artist, record companies, and the consumer. Fairplay allows a purchased song to be played on up to five computers, to be included in a playlist up to seven times, and to be burned an unlimited number of times [9]. The absence of this DRM will prevent the RIAA from licensing content to Apple for use in iTunes Store. The iTunes Store is also a significant investment on Apple's part, and Apple would like to see a return on their investment either through purchase of music or purchase of hardware to play the music. The Fairplay DRM also keeps the iPod, Apple's digital music player, as the sole supported device of the iTunes Store. Those who reverse engineer the DRM scheme or use tools which reverse engineer the DRM scheme in order to use the media on another device could be subject to prosecution under the DMCA. Users have found a way around the DRM protection by burning the audio to a CD, then ripping the CD and compressing the audio as an MP3 (or other format) without any of the restrictions of Fairplay. Perhaps this suggests that Apple may not be too serious about DRM as they allow such a loophole? Some thoughts are that Apple may have included the

DRM scheme to appease the RIAA, that they may intentionally have included the loophole for whatever reason and intend to tighten control later in time, or that Apple does not think the market will accept DRM without a loophole or reasonably convenient method around it at present [73].

Other companies are unwilling to deal with loopholes in their products. Some companies are suing those who break a particular DRM scheme and try to profit from breaking restrictions. For example, Lexmark corporation has used the DCMA in order to prevent third parties from manufacturing ink cartridges for Lexmark printers. In a lawsuit filed in December 2002, Lexmark claims that Static Control Components violated the DMCA by selling its Smartek chips to companies that refill toner cartridges and undercut Lexmark's prices [40].

> The company claims the Smartek chip mimics the authentication sequence used by Lexmark chips and unlawfully tricks the printer into accepting an after-market cartridge. That "Circumvents the technological measure that controls access to the Toner Loading Program and the Printer Engine Program," the complaint says. The Toner Loading Program checks toner levels in the cartridge, and the Printer Engine Program controls operations such as paper feed and the actual transfer of the dry ink to paper[40].

Section 1201 of the DMCA states that it is unlawful to circumvent technology that restricts access to copyrighted work, which Lexmark claims is broken by Smartek [40]. Unfortunately, this means reverse engineering for the sake of interoperability between companies is not allowed.

The Electronic Frontier Foundation (EFF), a civil liberties group based in San Francisco, seems to think that DMCA is meant for anti-competitive uses. Additionally, the EFF is one of the chief critics of the DMCA. Cindy Cohn, an attorney at the Electronic Frontier Foundation, expects more cases preventing interoperability like the one brought by Lexmark. "We have long said that the DMCA's potential use as an anticompetitive tool has been great," Cohn said. "Now we're seeing it happen." [40]

The EFF is also critical of DRM, saying DRM technologies may be used by copyright owners to erode capabilities that had previously been permitted to the public by copyright law under the "fair use" doctrine (or its cousins, such as first sale or limited term) [72]. It that their view of DRM and the DMCA are that they go hand in hand, where DRM contains the eroding capabilities and the DMCA is a law which prevents cracking DRM to remove the restrictions.

Microsoft Corporation, one of the largest software producers in the world, has included activation in its recent products. From their website, they claim that their product activation is:

> An anti-piracy technology designed to verify that software products have been legitimately licensed. This aims to reduce a form of piracy known as casual copying. Activation also helps protect against hard drive cloning. Activation is quick, simple, and unobtrusive, and it protects your privacy [11].

Thus, Microsoft claims that activation is intended to reduce piracy. This could in fact be accurate, as their Windows software is known to be pirated by many people, as well as their Office software suite. Additionally, one could argue that Microsoft has become so popular as its prior versions of software did not have anti-piracy measures while its competitor's products did, and now Microsoft is moving away from the model which made them successful.

According to Howard Stringer, Chairman and Chief Executive Officer, Sony Corporation of America,

> DRM allows us to tailor our copy protection to individual media, individual content, and different types of devices. It allows content companies to create new business models and allows consumers to choose the terms of usage whether based on time, copying rights, type of media or other variables of consumption. It should be easy for consumers to understand. And easy for them to use [61].

The above statement is vague. It does not explicitly say that Sony's DRM is to prevent piracy. It does say that DRM allows content companies to create new business models, perhaps ones that use the Internet for distribution instead of physical media. Also, Stringer says consumers can choose the terms of usage they feel appropriate but does not mention anything about the types of terms that may be available. This seems to indicate that the chairman of Sony believes DRM will be a requirement for doing business in the digital age.

Universal Music, the World's largest music company [30] says it will use a digital music format in order to allow for digital commerce, but it will use a DRM format that "will provide protection for artists' rights." [30] What exactly is meant by "protection for artists' rights" is not clear, and that could range from freely allowing music to be distributed to restricting or eliminating music distribution. From the statement, it seems Universal Music also feels that DRM is a key component of doing business in the digital age.

5.1.2 Should we trust the corporations proposing DRM?

We begin by considering an example in which Sony Corporation violated the trust of the consumer. Sony released CDs in the Fall of 2005 that contained software to play audio content on a consumer's a PC. This software secretly contained a rootkit in addition to the desired software. A rootkit is software which infects the operating system and conceals its existence from the user. Usually, a rootkit is inserted with a malicious intent. The following clip from an online news site explains exactly what Sony's rootkit software does.

> Sony BMG Music Entertainment distributed a copy-protection scheme with music CDs that secretly installed a rootkit on computers. This software tool is run without your knowledge or consent – if it's loaded on your computer with a CD, a hacker can gain and maintain access to your system and you wouldn't know it. The Sony code modifies Windows so you can't tell it's there, a process called 'cloaking' in the hacker world. It acts as spyware, surreptitiously sending information about you to Sony. And it can't be removed; trying to get rid of it damages Windows [53].

From this excerpt, we see a massive invasion of privacy as the software modifies the Windows operating system without telling you. It secretly spys on you by gathering information about your music habits and sends that information to Sony. Why does Sony want your music habits? Perhaps to target music advertising specifically for your taste, thus increasing the chance you will make a purchase. Further compounding the problem, the rootkit can not be removed without damaging the operating system. The EFF has a list of the CDs infected by the rootkit. The EFF also provides a method to identify them [74].

Another example of abuse of trust from the media corporations is on DVDs and the User Operation Prohibition (UOP) flag. The UOP flag was intended to prevent the user from skipping parts of the DVD, with the intent to prevent copyright notices from being skipped. Some DVD publishers have marked commercials (or previews) at the beginning of the disc with the UOP flag, thus preventing them from being skipped. One example of such abuse is found in the DVD for "The Sixth Sense". [70] This abuse of the UOP flag, using it to force consumers to watch commercials or previews, instead of using the flag as intended, is an egregious violation of the trust given to media companies by consumers.

Another example of mistrust from the corporations, again related to DVDs, is that DVD playback was not initially possible on Linux boxes. After a few years with no supported playback software, people in the hacker community took it upon themselves to write playback software. They first had to break CSS, which they successfully did with a program called DeCSS. With DeCSS published, the last hurdle of DVD playback on Linux was removed, and software for playback was produced. Playback of DVDs on Linux is something that should be considered fair use, as the content was legally purchased but was not able to be viewed. However, the RIAA response to the DeCSS algorithm was a series of lawsuits, suing the author of the algorithm as well as those sites distributing the algorithm [64].

5.1.3 Does DRM have the potential for abuse?

Now that we have explored the corporation's views for the introduction of DRM, we should examine if it is possible to be too restrictive with DRM. Is it possible that DRM has the potential for abuse?

The EFF, a major opponent of DRM, says "DRM technologies may be used by copyright owners to erode capabilities that had previously been permitted to the public by copyright law under the "fair use" doctrine (or its cousins, such as first sale or limited term)" [72]. Additionally the EFF says it seems unlikely that any DRM technology, or at least one that will be embraced by the copyright industries for their products, will be able to accommodate the full range of fair use [72]. This means they feel any DRM adopted by mainstream companies will prohibit some of the fair use clauses that were accepted, such as resale and being usable for a limited length of time.

The EFF also warns that the erosion of fair use with DRM has the potential ramifications:

- A reduction in freedom of expression, to the extent DRM interferes with review, commentary, scholarship, and parody

- A reduction in innovation, to the extent that DRM eliminates the reservoir of incentives that spur companies to develop technologies that interact with copyrighted works

- A reduction in innovation, to the extent that DRM depends on legislative mandates (whether in the form of the DMCA, a mandate from the Broadcast Protection Discussion Group or the pending Hollings bill) that interfere with science and technology development

- An erosion of privacy, to the extent that DRM compromises user anonymity
- The "freezing" of fair use, to the extent that DRM systems will prevent courts from evolving fair use in response to new technologies
- Undermining archives, libraries, and others who store and preserve our cultural heritage, to the extent DRM systems prevent free archiving of copyrighted content
- Lessened competition, to the extent that DRM systems prevent companies from engaging in legitimate reverse engineering of competitors' products. [72]

From a development standpoint, if software such as iTunes is able to prevent downloading music to music players other than iPods (via their FairPlay scheme), how difficult is to prevent them from one day preventing users from burning downloaded music to CDs? Currently, as technology limits the number of computers which are allowed to play back the music, it would be fairly easy to prevent any computer from playing the media without an additional fee, such as a renewal fee. What is to stop the inclusion of payment for each time a file is accessed, other than consumer revolt? Alternatively, what stops them from allowing consumers to be happy by not restricting the media they purchased? At the moment, the media companies are happy getting revenue from consumers who purchase music. If the companies feel it is financially beneficial to implement the aforementioned restrictions, we may start to see them.

The artificial locks used by DRM could easily change if the device is able to connect to the internet. DRM can change either to tighten control or to loosen control, at the decision of the DRM authors. At present, there is nothing to stop corporations from changing policies at their own discretion, and to the surprise and detriment of the end user.

Another idea is based on Trusted Computing (TC). The only software that is authorized to run is software that has been approved by the maker of the operating system or the hardware manufacturer. The question is, what stops the approver from only approving software made by that particular corporation, thus in turn creating a virtual monopoly? Or, who maintains oversight of what is approved so artificial vendor lock in does not occur?

The Sony rootkit incident is an example where the corporations have violated the trust of the consumer. The affected CDs contained software which misled the user as it contained spyware while not stating its true purpose. Additionally, the fix from Sony to remove the spyware from affected computers contained additional spyware. This leads the consumer to be skeptical about motives of corporations, as the rootkit incident shows the corporations can not be blindly trusted.

For consumers to fully trust the new DRM technologies proposed by corporations, there must be a system of checks and balances to ensure abuse does not occur. Without a system of oversight, the corporations could potentially abuse their power. Oversight would mean changes in technology and policy are approved by an oversight group. Additionally, the oversight group may reject changes that are unreasonable.

When the US government was formed, a series of checks and balances were put in place to prevent any one of the three branches of government from obtaining too much power. Unfortunately, the current DRM schemes do not have any such checks or balances, thus theoretically corporations could do whatever they want. How can we ensure that corporations who implement DRM do not abuse their power? How can consumers be sure they will not be locked into a particular vendor? How can anyone assure fairness with DRM? Without any oversight, how can consumers be sure they are getting the product for which they paid.

Open source software inherently has oversight, as anyone can examine the source code. However, closed software and closed technologies, such as DRM and Trusted Computing, are similar to a black box as the functionality is implemented but the public can not look inside to examine how the functionality was implemented. Verification of functionality and proof that a black box does what it states and nothing else can occur only if an independent reviewer has access to the inside of the black box.

A system of oversight governed by the consumers would be required in order to protect consumers. Consumers can already vote with their wallets by purchasing content with DRM that they deem acceptable. However, when all vendors offer similar restrictions, consumers have no choice. A system where the majority of consumers determine the restrictions on upcoming media formats would be appropriate. This would allow consumers to contribute to the development process of new technologies. A system of oversight would encourage hardware and software manufacturers to fully disclose what their technologies do. Additionally, consumers would be ensured that their privacy is not breached, security issues are minimized and resolved in a timely manner, and that the consumer's trust is not violated. Thus, technology should either be open for the public to examine or there must be an oversight group.

Based on the discussion above, it is entirely possible that DRM can be abused. The creation of an oversight group to inspect new technologies and DRM policies would be beneficial to the consumer and would help restore consumer's faith in the corporations. Now let us examine whether DRM is primarily a method to reduce piracy.

5.1.4 Is DRM a reaction to piracy? If not, why is DRM included?

In a prior part of the paper we have discussed that some corporations publicly state the inclusion of DRM and similar technologies is to combat piracy. This may in fact be their stance, but it is wise to explore if there may be an alternate reason for including DRM. Often it is one thing to state something publicly but another thing to actually remain true to the words.

For example, in the Sony Rootkit case mentioned previously, it is known that the rootkit installed by Sony contained code to monitor users, then send that data to Sony without the user's consent. Why did Sony feel the need to monitor users? Did it feel users were too inclined to pirate, thus felt the need to snoop on them? Why did Sony not tell users about this, instead of secretly installing the software? Is the data sent to Sony stripped of any personal information, or can Sony identify individual people? It is known that some websites use cookies to track people's surfing habits, send that information to a server, then produce ads targeted at the particular user. Was DRM and the rootkit really intended to prevent piracy, or was the real intent to collect data, then try to target specific advertisements towards users? The above action seems to question whether DRM really was used for anti-piracy measures or for something else.

Next, let us examine the motivations behind Trusted Computing. On the Internet, speculation for an ulterior motive for Trusted Computing can easily be found. The EFF states that even if third party software meets the specifications required by the TCG (Trusted Computing Group), the software may not necessarily be allowed to run on the computers. This would in effect create a virtual monopoly by locking all third parties out. This reduces freedom of choice, and in effect, would force the user to purchase all software from only the approved vendor(s). Due to virtual monopoly status, there would be no incentive to keep prices on software low, thus allowing the corporations to price software artificially high due to the suppression of competition. This in turn would mean huge amounts of revenue for a few years (until replacement hardware without TCG became available) [54]. The TCG is already using its technology to help cellular phone carriers lock down phones. For example, two clauses "Device integrity" and "SIMlock/device personalization", would prevent users from being able to switch carriers without purchasing a new phone. Two others clauses, "Platform integrity" and "software use" allow a virtual monopoly on which software is allowed to run on phones, thus making it impossible to use software not sanctioned by the carrier. The EFF article about Trusted Computing goes on to list a few more potential risks, and can be viewed at their website [54].

5.1.5 What do consumers think?

Next we examine consumer reaction to DRM. The first thought concerns Apple's iTunes Store. The restrictions in Fairplay may be reasonable to consumers, thus it may be one contributing reason as to why the iTunes Store is the most used digital music store. It should be noted that the iTunes Store sales are driven in part by the amount of iPods sold and people wanting to use the service guaranteed to work with the iPod.

With regards to software activation by Microsoft Corporation, consumers have been quite keen on using pirated versions of software which do not include activation. Patches can easily be found on the Internet which disable the activation, and instructions on how to apply them can also easily be found. Additionally, a search using the keywords "Windows no-activation" turns up close to 10,000 results on Google's search engine, meaning people are actively posting methods to circumvent the activation found in Windows. This shows that consumers, while wanting to use popular versions of software, do not want to deal with the activation method in that software, and are taking measures to circumvent activation.

With regards to Circuit City's DiVX experiment, their competing format to DVDs, Circuit City's format eventually was pulled. Consumers probably did not like the idea of having to pay to watch the movies they purchased, even if the long term cost would be less than purchasing the movie on the DVD format. Due to the lack of consumer interest and lack of sales, Circuit City eventually had to cancel the format. In the end, Circuit City decided to allow all the DiVX content to be viewed anytime for no cost.

5.2 What is the effect of DRM on the end user experience?

Next we will try to see what effect the digital restrictions in DRM may have on the end user experience. From this we can start to learn whether DRM will benefit or harm the end user.

Advantages and Disadvantages

The main advantage of DRM is that DRM reduces piracy, and a reduction in piracy means the user has high quality, genuine content. According to the RIAA, reducing piracy will help the consumer as the RIAA has more money to pay artists, which in turn will bring in new artists. Additionally, DRM removes the ambiguity on what is legal and illegal to do with purchased content. Therefore, people would not have to worry about lending music to their friend and hoping not to get caught, as the DRM would make it difficult, if not impossible, for the other person to use the media. Thus, the use of DRM would reduce copyright infringement.

Some of the bad reasons for DRM are that it could force the end user to only use certain hardware to play certain media. We see this already with music from the iTunes Store only being able to play on Apple's portable music players. DRM could also embed instructions to stop working after a period of time and only be allowed to work if new hardware was purchased. This would lead to an artificial lock in to a manufacturer. Another bad aspect would be that DRM may prevent getting updates. DRM may force consumers to purchase a new version of the software or media, where in the past a consumer may have been able to get software updates for free or transcode their media to new formats.

Control of Access

A major reason the end user experience could be affected (positively or negatively) is the matter of who sets the controls of the DRM. The corporations want to set the rules, being the producer of the content, while the user has no control over this. In effect, the user is at the mercy of the corporations, as they would have no say in the controls of the content they purchased. With corporations setting the rules, there would need to be a system of oversight to make sure the media companies do not produce a virtual monopoly and eliminate competition.

Will users be required to purchase new hardware to play content?

With any new media format, a new piece of hardware must be purchased in order to take advantage of it. However, with DRM, some existing components may need to be replaced with new, DRM enabled versions. For example, a receiver that has some form of DRM embedded in it may only allow certain DRM formats to play on certain 'DRM approved' speakers. A new format may force the purchase of new speakers just to play a new format just to satisfy the receiver. This example would force the user to purchase a new set of speakers prematurely, in a sense the user would needlessly spend money, just to be compliant with new restriction standards.

Another example concerns trusted computing, where the power leveraged by the computer manufacturer may be used to prevent software made after a certain date to be installed or function, thus forcing the purchase of a new computer. Often times special DRM formats have a special player associated with them, but in order to be accepted by the market they may include support for similar or rivaling formats. In this case, a computer may shut off or refuse to work after a certain date, preventing it from being used in a secondary role. Often times a collection of donated computers is used to set up an educational lab. DRM may prevent these computers from operating at their full, educational potential.

A third example is the High-Bandwidth Digital Content Protection (HDCP) format proposed by Intel Corporation. This format would prevent computer monitors that are not approved to be rendered unable to play certain signals, but not because of any technical limitations. It is likely that media with such restrictions in it may only play on an approved list of video cards, potentially forcing the user to have to buy two or more new pieces of equipment. The HDCP format dictates that high definition digital content will be reduced to DVD quality if passed through non-HDCP outputs, and audio that is not passed through HDCP outputs is reduced in quality. The idea is to prevent recording of the high definition, high quality content in the intermediate stages. This would render the current high end, expensive displays on the market useless as almost no devices on the market support this standard [69].

Limiting the number of times a user can burn/copy/distribute content

Another reduction in the amount of freedom may come from being artificially limited to the number of copies that can be made by media with DRM. Legally, people are allowed to make copies of purchased media for backup purposes, but the inclusion of DRM that prevents copying could prevent this use which is protected under 'fair use'.

Apple's Fairplay already limits the number of times a song can be used in a playlist, but does not limit the number of times a song can be burned to CD. Additionally, Fairplay restricts the number of computers which are allowed to play a purchased song.

5.3 Impact of DRM on society

This next section describes the potential social impact that various restrictive technologies would have on society. To start out, the discussion starts with software licenses, a very hot topic in the computer industry.

5.3.1 Software Licenses

Software licenses are important as they determine how people can use software, as well as potentially govern distribution of software. Currently a variety of software licenses exist, ranging from being very restrictive to very open. An example of a very open license is the Berkeley Software Distribution license (BSD) which essentially places all content under its license in the public domain [63]. Another popular license is the GNU General Public License (GPL), which grants the recipient of computer software the following freedoms:

- The freedom to run the program, for any purpose.
- The freedom to study how the program works, and modify it (access to the source code is a precondition for this).
- The freedom to redistribute copies.

- The freedom to improve the program, and release the improvements to the public (access to the source code is a precondition for this). [25]

In addition to being a software license, the GPL is also a philosophy about sharing, freedom, and open access to the source code of a program. The GPL allows one to do what they want with the program and source code and release improvements as they see fit. This license and the BSD license allow for people to trade software without worries of breaking any laws or infringing on anybody's copyrights. The numerous Linux based operating systems are a testament to how popular the ideas of the GPL are.

Other licenses, such as licenses set up by commercial companies like Microsoft very clearly prohibit sharing of software. Such sharing is seen as piracy by them and is subject to prosecution [15]. This means if your friend comes over to see your new software and likes it, you can not give him a copy without breaking the law. If the friend really wants a copy of the software, you could potentially be put in a difficult situation, deciding whether to strain the friendship or make a copy, break the law, and hope not to get caught. This type of distribution is prohibited as the software vendor does not receive any payment for their work.

GPLv3

The Free Software Foundation, writers of the popular software license GNU Public License (GPL), have made a provision in their third revision of the GPL that addresses DRM. While currently in its second draft, it has caused some commotion among the industry. For example, take the following excerpt:

> Some countries have adopted laws prohibiting software that enables users to escape from Digital Restrictions Management. DRM is fundamentally incompatible with the purpose of the GPL, which is to protect users' freedom; therefore, the GPL ensures that the software it covers will neither be subject to, nor subject other works to, digital restrictions from which escape is forbidden [25].

While this does not directly mention the DMCA, it is clear that the DMCA is indirectly addressed by this statement. In section 1, paragraph 3, of the new version, GPLv3, says:

> Complete Corresponding Source Code also includes any encryption or authorization codes necessary to install and/or execute the source code of the work, perhaps modified by you, in the recommended or principal context of use, such that its functioning in all circumstances is identical to that of the work, except as altered by your modifications. It also includes any decryption codes necessary to access or unseal the work's output [60].

This means that all information required to run the software must be included in the source. For example, if a special key is needed to run or decrypt hardware, that key must be provided in the source code of the software, otherwise the software is in violation of the GPL [60]. The inclusion of the mechanism to circumvent any of the restrictions seems to somewhat defeat the purpose of inserting them in the first place. Software which is licensed under the GPLv3 can not be used to create or insert DRM into products.

If the GPLv3 license is adopted by the open source community, this could have major impacts on current and future products which contain open source software. Products which contain software licensed under the GPLv3 must either forgo the use of DRM, or use alternative software. Additionally, open source software released under this license will automatically be limited to use in devices which do not implement any form of DRM.

For example, if the open source software used in Tivo is released under GPLv3, the makers of Tivo would need to either forgo using DRM. If they chose to keep DRM, they can not take advantage of any improvements in open source software that is licensed under GPLv3. Additionally, there are various other consumer electronics which use open source software, such as cellular phones, personal digital assistants, and cameras. A switch to the GPLv3 license would make it more difficult for these types of devices to include DRM. In addition, GPLv3 software could not be used to develop or implement newer versions of DRM technology.

5.3.2 DRM restrictions on the use of purchased material

Restrictions imposed by DRM could have an impact on current behavior of society. Currently, if a friend wants to borrow a movie or CD, they are able to borrow it as long as the owner is willing to loan it. Many times the friend ends up liking the media enough to go out and buy their own copy.

With the inclusion of DRM, only the owner of the content would be allowed to play back the media. Using the previous example, a friend could again borrow the content, but since the friend is not the owner, the DRM would prevent playback for the friend. Additionally, if the DRM has some instructions to connect to a central server on the Internet, both the owner and the friend could be reported as pirates and be prosecuted.

Additionally, there are cases where a backup legitimately needs to be made. With DRM, a restriction on backups may prevent this, thus angering the consumer who may wish to protect against accidental loss or corruption.

Lastly, with the restrictions imposed by DRM, transcoding, the digital-to-digital conversion from one format to another, could be stopped. Currently, a person who has purchased an album on CD is able to rip the music and convert it to MP3 for playback on their portable digital music player, as well as store the album in a variety of other formats. Similarly, the owner of an MP3 file could transcoded the audio file in any new audio codec, such as Ogg Vorbis, AAC, etc. With DRM, the restrictions would prevent the media file from being transcoded into different formats, eliminating the possibility of playback of the file on different devices. The DRM would then make it easy for the media companies to charge consumers to have a copy of the media in each format, such as one charge for use on the computer, one charge for use on a digital music player, and another charge for playback on a different device such as a Personal Digital Assistant (PDA).

These restrictions would impact society as they would prohibit behaviors which are currently permitted. If a content owner is the only person who can play back media, then nobody else would be able to play back the media, not even friends or family. This may potentially reduce sales as content may get less exposure. Additionally, a copy for backup purposes could not be made, forcing consumers to potentially re-purchase or pirate content they already had obtained. This could potentially anger consumers and also potentially increase piracy. Lastly, the restrictions on transcoding legally purchased content may prevent new devices for content playback from gaining popularity, as less content would be available for any particular device, potentially hurting innovation and lowering hardware companies.

5.3.3 Laws passed relating to DRM

This next section discusses laws that have been passed and rulings issued that are relevant to DRM in the United States. The first ruling is regarding the Betamax Court case, where the US Supreme Court eventually ruled time shifting of video is legal in the US.

Betamax Court Case

In the mid 1970s Universal Studios and Disney Corporation became wary of video-recordings. In 1976 they decided to sue Sony Corporation, makers of the Betamax video recording hardware. The claim was that the devices could potentially be used to for copyright infringement and Sony was liable for any infringement committed by its purchasers. Many years of court battles entailed culminated with a supreme court ruling.

In 1984, the Supreme Court ruled in favor of Sony and determined home videotaping to be legal in the US since they had substantial non-infringing uses. Additionally, the court said about Betamax in particular:

> The question is thus whether the Betamax is capable of commercially significant non-infringing uses ... one potential use of the Betamax plainly satisfies this standard, however it is understood: private, noncommercial time-shifting in the home. It does so both (A) because respondents have no right to prevent other copyright holders from authorizing it for their programs, and (B) because the District Court's factual findings reveal that even the unauthorized home time-shifting of respondents' programs is legitimate fair use....[16]

Thus, with this ruling, the court ruled in favor of Sony. It also said that private, noncommercial time-shifting of content is fair use. The Betamax format did not have DRM in it, but the 1984 court ruling which emerged from Sony and Hollywood's battles set the stage for later rulings.

DMCA

There are no direct laws which indicate DRM is legal or illegal. However, the Digital Millennium Copyright Act (DMCA) prohibits the reverse engineering of software. This law, while not passed specifically for DRM, has been used to help the corporations justify their lawsuits. For example, the DMCA has been used to stop the distribution of the DeCSS algorithm, which allows copying of commercial DVDs, within the US, with hosts receiving cease-and-desist notices from lawyers.

This law prevents any legal reverse engineering of DRM, hardware, and algorithms, even reverse engineering for interoperability. With this law, companies are unable to produce a product which may operate with another company's product without using a published specification. This law potentially stifles innovation as companies could potentially be sued or shutdown.

FCC Ruling on broadcast flag

The broadcast flag is a bit (or series of bits) called a flag in a digital television (DTV) signal. The purpose of this flag is to specify whether the stream is able to be passed to unauthorized digital tuner hardware or copied by digital recorders, such as any personal video recorder. The Federal Communication Commission (FCC) mandated the broadcast flag be incorporated in all TV receivers using the ATSC standard by July 1, 2005 [62]. However the DC Court of Appeals overruled the mandate in May 2005, saying the FCC lacks the authority to try and impose such a rule [57].

Is the United States forcing other countries to impose laws such as DMCA?

The United States may be suggesting other companies impose laws similar to the DMCA in order to gain economic benefits. Laws which are similar to the DMCA now exist in parts of Europe (EU Copyright Directive), in Japan, and in Australia. According to the IEEE, a professional society for Electrical Engineers, nine more countries have been pressured into passing DMCA like laws as US trade negotiators say copyright change in other countries is necessary to secure free trade pacts with the US. Additionally, a European body in charge of defining the European Digital Television standard is mixing in content-protection schemes, responding to pressure for Hollywood movie studios [38].

5.3.4 Educational Institution Responses to piracy

Worcester Polytechnic Institute (WPI) has reacted to RIAA lawsuits targeting students by locking down their campus network. Any violation of the WPI Acceptable Use Policy (AUP) is noted and the student notified and instructed to remove the copyrighted file. The Network Operations (NetOps) staff, who are in charge of maintaining WPI's network, actively search users shared folders and try to find copyrighted material [71]. Additionally, NetOps prohibits any file-sharing with peer-to-peer (p2p) software within the campus and outside the campus since they have found most material on these networks violates the WPI AUP. Their stance is to shut these activities down in order to protect students and the university from potential lawsuits [71].

In 2003 the Massachusetts Institute of Technology (MIT) was issued a subpoena by the RIAA for names of students who were sending out copyrighted material on the Internet. MIT's Vice President for Information Systems James Bruce responded by saying the Family Education Rights and Privacy Act (1974) prevents them from disclosing these names except under certain conditions. Regarding the special situations, he said "One of the situations is when an educational institution is served with valid subpoenas." [52] Lastly he said that MIT has been advised by their counsel that the RIAA subpoena did not comply with court rules which apply to subpoenas, thus they would not honor it [52].

5.3.5 Social and Ethical Relationships

The next sections takes a look into some social and ethical relationships amongst humans. DRM may lead to some social problems, as the restrictions may interfere with the way humans normally act. For example, with past formats a friend could ask a friend to borrow media, do what he desired, then return it. With DRM, it may be next to impossible for borrowed content to be played by someone, as the DRM restrictions may prevent it. Additionally, DRM may make it easier to catch those who lend content, and this would leave the friend in a conflict between being law abiding and trying to be social.

Stanford Prison Experiment

The 1971 Stanford Prison Experiment experiment is a famous psychology experiment which took place at Stanford University and simulated prison conditions. It showed how ordinary, educated citizens were capable of doing harmful things they would have never believed they were capable of doing. Several people were selected to be inmates, and others were selected to be guards and instructed to keep control of the prison without using violence.

Stanford Psychology Professor Philip Zimbardo recalls:

> I had been conducting research for some years on deindividuation, vandalism and dehumanization that illustrated the ease with which ordinary people could be led to engage in anti-social acts by putting them in situations where they felt anonymous, or they could perceive of others in ways that made them less than human, as enemies or objects.

At the start of the experiment, guards' aggression towards the inmates was minimal, but quickly increased to the point where the experiment was called off after only five days; it was originally planned to be a two-week experiment. To summarize, the findings of the experiment were that there was some truth to demonstrate the impressionability and obedience of people when provided with a legitimizing ideology and social and institutional support [48]. In other words, it seems that ordinary people are capable of being disobedient and extremely violent when placed in a position of power.

Perhaps the finding that people may not behave as expected when put in a position of power has parallels in entertainment industry. It is possible that a few people in control are able to run several corporations as they desire, and that desire might be to extract as much revenue from the customer base. Restrictive technology such as DRM could be implemented so media companies receive as much revenue by forcing consumers to purchase content as many times as possible.

Milgram Experiment (Shock Treatment at Yale)

Another famous psychology experiment was the 1961 Milgram experiment at Yale University. It tested people's obedience to authority when instructed to do something which may conflict with their conscience. The experiment worked by having three people, in which the teacher tried to teach a series of word pairs to the learner who is located in a separate room, and an experimenter watching the teacher. If the learner correctly learned a word pair, the teacher went on to the next word. If the answer was incorrect, the teacher would shock the learner, with the shock voltage increasing with each wrong answer. In reality, there were no shocks, just tapes which would play in order to simulate a response to a shock [41].

After a series of increasingly intense shocks, the teacher would question the purpose of the experiment and express a wish to stop. The experimenter instructed the teacher to continue the experiment, and the teacher would continue, however the experiment stopped after the teacher's fourth desire to stop. If the teacher did not express four desires to stop, the experiment ended with the subject getting the maximum shock three times in a row. This experiment showed that ordinary people are willing to obey an authority who instructs them to do something which may go against their conscience.

This conclusion could be dangerous, as it may mean the people running the media companies are able to do what they desire while artists and consumers are too slow to express their true thoughts. Consumers may not speak out against technologies they feel are inappropriate or a violation of their rights immediately, and it may be too late when they do speak out. Consumers may not realize they need to speak out immediately if they are against a technology, especially if they feel their rights are being encroached.

Share music with friends?

Seeing the previous two experiments, one can start to wonder how this would lead to interactions among humans. Just to think, if people feel DRM is bad, how much will people put up with it? From the Milgram experiments, people tend to follow orders even if they go against their conscience, which could be bad as it could cause people to be more closely follow the law as corporations tell them what they can and can not do with the content they purchased. If DRM turns out to be too restrictive and consumers decide to revolt, people may not be vocal enough in their anti-DRM thoughts, and perhaps it would be too late before people took action against DRM.

5.3.6 Social Behavior of People

The insertion of DRM would definitely make media lending difficult, as the owner of the content may be scared of legal ramifications. Also, if the person actually receives the media, they may have to break the DRM, leaving that person open to prosecution if caught. The thoughts of people may be such that they think just a single violation of the copyright law will result in prosecution, or the opposite, that they can pirate as much as they want and never get punished for breaking the law. Some people may be against pirating not for legal reasons, but because they feel it is wrong. Lastly, other people may feel that pirating content is quite alright, and may not think anything of it when committing piracy.

It would be incorrect to say nobody shares music with their friends. However, not everybody shares music either. Some people do, but the number who share music has not been determined nor is it necessarily easy to determine. Before digital music was common, people definitely did share their analog music, but it was tougher to share as a physical distribution network was required. The difficulty of setting up a distribution network could be debated as people often go visit friends, and thus could potentially bring media along with them. We could speculate why people shared music, such as to spread the word about new, upcoming artists, to show off new hardware they just purchased, to let a friend decided about purchasing the work, or even just because they want to share music.

The inclusion of DRM could alter social behaviors since corporations are telling consumers it is bad to share. People have been sharing various items for various reasons, and sharing media could potentially be beneficial. However, the inclusion of DRM to reduce sharing, with the threat of prosecution, implies the corporations feel sharing is bad. Consumers may start to feel guilty when sharing media, and this feeling could potentially reduce sharing other items.

5.4 Is DRM the solution to stop piracy?

This next section explores whether piracy is as big a problem as the media companies suggest it is. Additionally, the idea of using DRM as a solution to piracy will be explored. To start out, the thoughts on the DRM advocates are presented, then the thoughts of DRM opponents will be presented.

5.4.1 What DRM Advocates Say

This next section present what groups who are for DRM have to say about DRM as the solution to piracy. This group consists mainly of media corporations.

RIAA and MPAA's Thoughts

The RIAA says piracy is a big problem. From their website, the claim to lose about $4.2 Billion to piracy each year [47]. Their website also lists a variety of reasons why piracy hurts the consumers, retailers, record companies, music pirates, and the artists. For example:

> Record companies lose. Eighty-five percent of recordings released don't even generate enough revenue to cover their costs. Record companies depend heavily on the profitable fifteen percent of recordings to subsidize the less profitable types of music, to cover the costs of developing new artists, and to keep their businesses operational. The thieves often don't focus on the eighty-five percent; they go straight to the top and steal the gold [47].

From that excerpt, it seems that the record companies need some way to reduce piracy in order to be able to cover the costs of bringing the music to the public. It is interesting to note that nowhere on their site do they mention anything about DRM.

The movie counterpart to the RIAA, the MPAA, says the following about piracy:

> Piracy is the single biggest threat to US Copyright industries in movies, home video, music, book publishing, periodicals, radio, television, video games and software. These Industries contribute to the US economy in job growth, contribution to the Gross Domestic Product (GDP) and Foreign sales and exports. In fact, The US Motion Picture Industry employs over 750,000 people nationwide, not to mention the thousands of peripheral jobs that rely on the movie industry such as advertising to popcorn manufacturers [46].

From their website, the MPAA seems to make a reasonable argument that piracy hurts everybody, in particular the people who are employed directly and indirectly as a result of this industry. Their main idea appears to be that if there was no piracy, there would be more revenue generated, and thus more people could be employed at various points.

Another description of piracy is given as:

> Piracy is theft, and pirates are thieves, plain and simple. Downloading a movie off of the Internet is the same as taking a DVD off a store shelf without paying for it. Posting it on a Peer-to-Peer (P2P) service or an unauthorized website is akin to giving illegal copies to millions of people [45].

The MPAA says that downloading a movie is akin to stealing it from a store. The moral and ethical issues regarding stealing from a store and downloading from a peer-to-peer network is a major topic by itself. Some folks feel downloading content on P2P networks is not akin to stealing as there is not physical media being stolen, such as walking into a store and stealing a DVD or CD from the shelf. Others feel the high prices and low perceived quality of the content are justifications for downloading, while still others feel that downloading content is in fact akin to stealing a physical copy from a store. Downloading from P2P networks is perhaps easier, as the requirements are a computer and an Internet connection, and the anonymity provided by the Internet may make people feel less likely to get caught than stealing from a store.

A part of the MPAA site is dedicated to what the MPAA claims it is doing to combat piracy. In it, suggestions for using legal methods of obtaining movies are given, such as using iTunes, Netflix, and Blockbuster. An excerpt directly from their site says how copy protection benefits the consumer:

> Copy protection benefits consumers as well as the industry because without these safeguards, the industry would not be able to release their high-quality digital content without the fear of widespread and rampant piracy. For instance, with PPV, because of the copy protection, there is a level of assurance that the movies won't be copied freely so movies can be offered at a very reasonable price considering the cost of making the product [44].

Giving the benefits of copy protection is understandable, but the website is not giving any more specifics on copy protection, such as what type of copy protection is used. The use of DRM in video and audio media is not mentioned at all, just the vague term copy protection is used. The consumers are very unclear as to how they may be trying to achieve this copy protection. Additionally, they do not mention any reason for copy protection other than the reduction of piracy, which in turn will lower the cost to the consumer. However, those consumers who do not agree with that argument may feel it is acceptable to pirate, as they may feel the reason for copy protection is flawed and the media companies are wrong, thus they protest by committing piracy and not paying for content. Their hopes may be that instead of paying the companies to continue with a flawed model against piracy, if piracy gets to a high level the companies will re-think their strategy against piracy and devise a better strategy.

DMCA

As mentioned in a previous part of this paper, the DMCA is a very tough law that essentially prohibits the act of reverse engineering or breaking any forms of copy protection. The MPAA, while not explicitly stating they use this law, seem to follow an approach that is consistent with exercising this law:

> The motion picture industry has pursued those who distribute devices that break copy protection in any format. While no technology has yet proven foolproof, the industry continues to implement protection technologies which raise the threshold of difficulty and expense for the pirate and therefore help reduce piracy [44].

Other examples of the DMCA being invoked are:

- In 1999, cease and desist letters were sent to people who hosted a copy of DeCSS on their website in the United States [23].
- Lexmark trying to prevent Static Control Components from selling remanufactured cartridges for Lexmark printers [40].
- IEEE revising its publishing requirements to make sure authors do not violate DMCA, potentially alienating a portion of their contributors [31].
- White House Cyber Security Chief Richard Clarke called for DMCA reform, saying it has hurt legitimate computer research [24].
- In September 2000, SDMI (Secure Digital Music Initiative) issued a challenge to remove watermarking intended to protect digital music. A professor at Princeton University took up the challenge, successfully broke the scheme, but was barred from presenting the findings as SDMI threatened the team under the DCMA [24].
- The shutdown of the website FedExfurniture.com by the FedEx Corporation in 2005, accusing the owner of the site of infringing on FedEx's copyrights and trademarks, and using the takedown provisions in the DMCA to remove the website [2].

Software Corporation's Thoughts

Microsoft Corporation, the makers of the Windows Operating system, gives the following reason for the need of DRM:

> Digital media files can be easily copied and distributed without any reduction in quality. As a result, digital media files are being widely distributed on the Internet today, through both authorized and unauthorized distribution channels. Piracy is a concern when security measures are not in place to protect content. Digital rights management enables content providers to protect their content and maintain control over distribution. Content providers can protect and manage their rights by creating licenses for each digital media file. License registration

> procedures also give these companies important customer information. Such information helps content providers stay closer to their customers. Having a robust DRM system in place ensures that a wide variety of the highest-quality audio and video content is made available to consumers [13].

Microsoft seems to feel that piracy is a concern and the way to combat it is by using DRM. DRM, as they say, allows creators to specify how each media file can have a separate license. Additionally, they seem to be in favor of having a registration processes, perhaps similar to their Activation in several of their software products, as they claim it gives companies important customer information. What types of information do they get, and why would they need customer information? Would they want to verify whether people who play the content have in fact paid for it? Would they be interested in finding out what the taste of their customers is, then targeting advertisements specifically for each customer? Would they try to prosecute those who play content and have not legally obtained it?

5.4.2 What DRM Opponents Say

This next section presents what groups who are opposed to DRM have to say. The first group, the Electronic Frontier Foundation (EFF) is a non-profit group who says their goal is to protect people's digital rights.

Electronic Frontier Foundation

The EFF says that DRM impinges on fair use. They say fair use and DRM are opposites, as fair use opens up new avenues of entertainment, while DRM potentially restricts new avenues. Currently, these new avenues are often found by a person who has an idea for a new regarding content, implements it, tells people and others like the idea and also start using it. New industries are often found this way. DRM would potentially inhibit the use of digital content for this sort of exploration, thus potentially hurting future industries. Additionally, these new industries often help strengthen or improve already existing industries.

For example, the advent of MP3s created a new industry in the late 1990s, mainly consisting of portable MP3 players and Internet music stores. It is possible that the desire to download music from digital music stores helped push sales of high speed Internet connections, however there is no direct evidence that this is the case. Additionally, it can not be difficult to imagine the amazing success of digital music stores as part of the reason for the opening digital movie stores, as is the case with Apple opening up a movie section on their iTunes Store. However, one could suggest that the technical means to distribute content without easily allowing piracy was not developed until recently, as current DRM methods make it possible for media companies to open online stores and feel assured their content safely distributed.

The EFF says the restrictions within the DRM will inhibit the growth of new industries, as the copyright owner must deem the new industry acceptable rather than the consumer [72]. This could potentially inhibit the creativity of someone who tinkers and accidently comes up with the next brilliant idea, as digital restrictions may inhibit that. However, the motivation and desire to do new things with restricted content may yield new industries as well. In another paper, the EFF says DRM has many unintended effects. They say:

- DMCA Chills Free Expression and Scientific Research
- DMCA Jeopardizes Fair Use
- DMCA Impedes Competition and Innovation
- DMCA Interferes with Computer Intrusion Laws [24]

The paper goes on to explain each bullet in great detail, giving various examples of corporations threatening to and often filling lawsuits in order to get their way. More often than not, the lawsuits end up stopping competition, hurting fair use, and even interfering with computer intrusion laws.

Free Software Foundation (FSF)

As mentioned in section 5.3.2, the Free Software Foundation's newest license, GPLv3, addresses DRM. The license prohibits software from being used to develop or implement DRM, meaning devices which desire to use DRM would need to find alternate software.

5.4.3 Is DRM a good way to reduce the piracy problem?

It is difficult to say if DRM is a good way to reduce piracy. Allowing piracy could be beneficial or detrimental for a company. It could be beneficial because little or no restrictions may make it easy to advertise a product. It could be detrimental if too much piracy significantly reduces profits.

For example, Microsoft Corporation initially released it software without any digital restrictions or activation. Consumers liked their software and were easily able to give it to friends, and those reasons, among others, allowed Microsoft to become so dominant in the software industry. One could make a case that if Microsoft had inserted the same means of digital restrictions as its competitors that it may not be as popular as they are currently since consumers may have been less inclined to purchase it.

Another thought is that if consumers do not want to purchase the media, then DRM may not be an effective countermeasure. For example, if a person has decided to download media, then all they need is a search tool to find a copy of that media which someone has made available. However, Cory Doctorow, a science fiction author and coeditor of the Internet blog 'Boing Boing', mentions the key point here is that the person has chosen to download the song, not purchase it, and no form of DRM could influence someone to purchase instead of download. Doctrow goes so far as to say the only way DRM could stop him from downloading is:

- Every copy of the song circulated, from the recording studio to the record store, had strong DRM on it.
- No analog to digital converters were available to anyone, anywhere in world, who might have an interest in breaking the DRM (since you can just avoid the DRM by making taking the analog output off the player and re-digitizing the song in an open format).

- Peer-to-peer networks ceased to exist.

- Search engines ceased to index file-sharing sites.

- No "small worlds" file-sharing tools were in circulation[18].

A quick look at the numbers shows that total album sales fell 7.2% in 2004, from 666.7 million sales to 618.9 million sales, according to Nielsen Soundscan. One might recall that 2004 was the height of the RIAA's cease and desist letters. Additionally, CD sales (95% of total album sales) fell 8.0% in 2004, from 651.1 million to 598.9 million. However, digital track downloads were a different story. They rose 150%, or to 352.7 million sales in 2004. Overall music purchases, which include albums, singles, music videos, and digital downloads, were up 22.7% and surpassed 1 billion units [3].

In October 2006, Brad Hunt, the Executive Vice President and Chief Technology Officer for the MPAA made the following statement: "I understand that if we frustrate the consumer, they will simply pirate the content." [10] He also mentioned that consumers are starting to become frustrated at having to buy multiple copies of content for use with different devices, and as a result are turning more towards piracy [26].

So, is DRM a good solution to piracy? Perhaps it is not, as suggested by Brad Hunt. Prior to the restrictions, consumers were able to purchase one copy of media and use it on any device they desired. However, with DRM preventing the open use of content, consumers are forced to either pirate content they already own or to purchase another copy for playback on another device. Consumers do not think too highly of purchasing content multiple times, thus are resorting to piracy [26].

5.4.4 Consumer sentiment about purchasing media

Many factors affect why consumers purchase music and video media. For example, a period of an economic recession would expect fewer purchases to be made than a better economic year, as during a recession people may be more frugal with their money. Another factor would be the perceived quality of the content. If there was a year with particularly few good movie releases or album releases, then it may makes sense that consumers are less likely to purchase. A year with a series of blockbuster or very popular albums would naturally increase the ratings.

In addition, many would be movie goers are finding it less appealing to go to theaters nowadays. Many consumers feel the price of tickets is quite high, in addition to feeling concession prices are outrageous. Lastly, many consumers also have their own home theater systems and many feel comfortable waiting until a DVD is released, rent it, and watch it in the comfort of their own homes. They find the whole movie experience at home is much better than at the local theater.

In addition to the above reasons, media sales may also be taking a hit due to rise of other avenues of purchase. For example, CD sales may be down, but album sales via online stores such as the iTunes Store may be higher than the loss the drop in CD sales. It is interesting to note that in 2003 and 2004 online music stores experienced phenomenal growth [3].

5.5 Does DRM really stop piracy?

Let us examine whether or not the inclusion of DRM in new products has actually lowered the piracy rate or not. In addition, let us examine some of the current DRM schemes and see how effective they were.

DVD's CSS was broken, allows DVDs to be ripped

The first example of breaking the digital locks was done in order to play DVDs. The Content Scrambling System on DVDs was broken by a teenager from Europe. The teen wanted to play DVDs on Linux, something that one would expect is fine under fair use, but the MPAA felt otherwise. While the initial use was legitimate, the breaking of the locks allowed for people to write software to pirate the DVDs.

Software product activation often defeated

people on the Internet have been able to reverse engineer almost all software to remove the CD checks, thus making this method essentially useless for those who use the pirated copies. In addition, some programs are available that can fool the program to thinking a mounted disc image is actually the physical media from a CD-ROM drive. Again, a quick search with google using the format "name of software + crack" will yield several results on any particular piece of software.

Microsoft's product activation for Windows XP and upcoming Windows Vista broken

The next example deals with software from Microsoft. Recently, Microsoft's popular software programs have included product activation. Often times, beta releases of these programs have been leaked to the hacker community via the Internet, which in turn has been able to defeat the activation schemes. Often the hackers are able to break the scheme within days of obtaining a copy of the software. To find specifics on these cracks, a quick search with google using "name of software + crack" will yield several results, ranging from instructions on how to manually crack and apply patches to links for torrents to download already cracked versions of software.

CD Copy protection methods defeated

The next example discusses how copy protection on CDs has failed. Over the years, various forms of copy protection have been introduced, and given time, have been broken. One of many popular formats, Macrovision's SafeDisc, has constantly been broken by common software, such as CloneCD. As each version of SafeDisc is released, the writers of popular CD copying software analyze the implementation and fairly quickly release an update which copies the disc. Another format, SecuRom, is used for software copy protection, but occasionally used for music CDs. The most invasive method used for music CD copy protection was surfaced in fall 2005 with Sony/BMG's rootkit fiasco which is mentioned in another portion of this paper.

iTunes Store copy restrictions broken

The next example is the music content purchased via Apple's popular iTunes Store. Jon Lech Johansen, the same Norwegian programmer who released DeCSS, was able to break the first iteration of Apple's DRM by paying careful attention to what files were written when a song was downloaded. Inspecting a particular key file led him to reverse engineer the encryption on iTunes Store purchased content. Johansen then released a program called PyMusique, a utility to strip the DRM from the downloaded content. PyMusique works by preventing iTunes from applying the DRM, essentially allowing the user to make a copy of the downloaded song. Apple responded by changing their iTunes Store code, and Johansen released an updated version to interface the new version of iTunes Store.

Rootkits

The Sony/BMG rootkit fiasco caused quite a headache for the recording industry. This event started on October 31st, 2005 when Mark Russinovich published details on his blog about the software contained on some Sony/BMG music CDs. His blog asserted the software was illegal since it installed itself without user authorization, had flaws in software design that contained security holes which could be used by viruses, and had no uninstall utility. The public outcry from the computer literate crowd was quite high, and under the pressure, Sony released a utility which they claimed would remove the rootkit component. Russinovich analyzed the utility and found the utility did not remove the rootkit, only masked it, and installed additional software. Again, the outcry from the people on the Internet was high, so Sony released what they called a new and improved uninstall utility. Finally on November 15th, 2005, Sony/BMG announced it was backing out of its copy-protection scheme, issuing a recall for affected CDs, and offering consumers to exchange the affected CDs for versions without the rootkit. The next day, November 16th 2005, US-Cert, part of the Department of Homeland Security, issued an advisory on the Sony/BMG DRM saying the rootkit was a security threat to computers. In addition, they also stated some very wise common sense:

> Do not install software from sources that you do not expect to contain software, such as an audio CD.

New York Attorney General Eliot Spitzer found through his investigators that on 29th of November, 2005 many retail outlets were still selling the affected discs. Spitzer said

> It is unacceptable that more than three weeks after this serious vulnerability was revealed, these same CDs are still on shelves, during the busiest shopping days of the year. I strongly urge all retailers to heed the warnings issued about these products, pull them from distribution immediately, and ship them back to Sony [37].

The next day Massachusetts Attorney General issued a similar advisory, also saying the affected CDs were still available in Boston. In addition, numerous class action lawsuits have been filed against Sony/BMG, such as on the 21st of November, 2005 when Texas Attorney General Greg Abbot filed a class action lawsuit on behalf of the state of Texas for illegal spyware [32]. Also on the 21st of Novembers, EFF announced they were filing their own lawsuit over the XCP and SunnComm MediaMax technologies. On December 20th 2005, the New York times stated Sony/BMG accepted a proposed settlement where those who purchased an XCP CD will be paid $7.50 per purchased recording and given the opportunity to download a free album, or be able to download three additional albums from a small list of recordings if they give up their cash incentive [35].

In summary, this event caused a lot of bad publicity for Sony/BMG. It is still rather early to tell if this event has scared consumers away from purchasing music CDs, but this event has shown the industry is not as innocent as they may make themselves out to be. The media coverage and quick actions of some stark Attorney Generals show the rights of the consumer are being defended in this case.

5.6 Examples of prior art using DRM

This next section describes some of the more recent DRM technologies found in consumer products. Some of the products containing these technologies have failed, while others have been very successful. The products which have already been discussed in detail in prior sections will be omitted.

DIVX

Digital Video Express (DIVX) was a format by Circuit City that attempted to create an alternative to video rental. It was released in 1998 just in time for the holiday season. The consumer was expected to purchase a DIVX capable DVD player, and to buy a DIVX disc for a few dollars. Upon first playing, the disc would be playable for up to 48 hours. After the initial 48 hours, the disc could only be played if the consumer paid a fee.

The idea was similar to video rental and the format was technically quite similar to DVD. DIVX also featured an encryption technology called Triple DES to prevent copying. Upon its release, Internet forums and home theater centric magazines called for a boycott of DIVX and to use "OpenDVD" instead. Consumers did not like the idea of DIVX, and on June 16th 1999, Circuit City decided to discontinue the format [36].

DVDs

When the DVD standard was being finalized in the mid 1990s, movie studios were well aware of the benefits of digital video quality and the potential ease of piracy, especially since digital content does not degrade in quality with copies. To counter this problem, engineers came up with a few solutions to help protect content.

The first anti-piracy solution was the Content Scrambling System (CSS). The descrambling of the video stream requires two keys, one unique to the disk and the other unique to the MPEG video file on disk. The keys are stored at the lead-in area of the disk and can only be accessed by compliant drives. The engineers came up with two reasons for CSS: the first to prevent byte-for-byte copies of the MPEG stream, and the other to force manufacturers to make compliant drives as the video would not play on non-compliant drives. In order to play a DVD, one would have to obtain a license.

The engineers realized that it would be possible to play the video and capture the analog stream. Thus, in order to prevent the capture of the analog stream, engineers used a second system called the Analog Protection System (APS). It allows signals to be displayed on the TV screen but unable to be recorded by VCRs as it tries to confuse the VCR's recording heads. An interesting note it that the APS is not contained in the actual digital video stream but is inserted afterward by the DVD player.

Next, engineers studied piracy and found pirated videos to be produced in one part of the world and exported to other countries. Thus, region codes were inserted. The idea was that DVDs purchased in one region would not play in another region, unless of course, the DVD was set to be region free. This was meant to cut down on piracy by making it more difficult for DVDs from one area of the world to be played by folks in another region of the world.

Other encryption methods were also implemented. The goal of the remaining methods was to ensure the secure transfer of keys from the DVD to the decoding device and to watermark the stream. These methods would make it difficult for someone to reverse engineer a DVD player's hardware in order to capture the keys required for decrypted playback [4].

Video Game Consoles

Recently console makers have expanded from their usual methods of copy protection on disc to using newer schemes. Sony Computer Entertainment America has implemented what they call the Dynamic Network Authentication System(DNAS). When games are played online, information about a user's hardware and software is sent to a central server for authentication, copy protection, account blocking, game management, and other purposes [1].

Flexplay

Flexplay is a name for a DVD format which is time limited. It usually makes itself unplayable after 48 hours. Once the package is opened, oxygen reacts with part of the disk, eventually turning it black. The company that is marketing this type of disks is called Flexplay Technologies. It is capable of being played in any standard DVD player. The target audience for flexplay was for promotional types of events and other short term uses and was hoped to succeed where other technologies such as DIVX failed [34].

Steam system from Valve

Steam is the content delivery, digital rights management, multiplayer, and communications platform developed by Valve Corporation for use with their Half-Life series of games. This content management system is used for a variety of reasons. When the user loads the game for the first time, the Steam system authenticates the game. Additionally, every time the game is loaded, Steam connects to the Valve servers and checks for 1) updates, and applies them automatically if needed, forcing the user to wait for updates to be applied, and 2) CD key is legitimate, warning and eventually disabling users who had invalid CD keys [27].

eBooks

Electronic books, called e-books, are digital forms of books commonly purchased in paper form from stores. Depending on the publisher, these digital books may have restrictions in them, such as limited or no printing allowed, viewing only on certain authorized devices, which could be as few as one. The cost of e-books may also play a factor in its success, as publishers are charging less for e-books, but not significantly less than paper versions. In addition, many feel paper versions of books have more advantages, as you are not tied to a device for viewing, can be signed by the author, and can reduce eye strain over time [75].

V-Chips

The last example, the V-Chip, is not DRM, but is an example of rights management. The V-Chip is a term for the feature which block channels based on their ratings. All televisions in sold in the United States since the year 2000 have V-Chips built into them. The ratings of television shows in the United States is based on the TV Parental Guidelines which went into effect in the US in 1997. This rating system classifies TV programs into various categories based mainly on the language, violence and intended audience. The idea behind the V-Chip is to allow parents the opportunity to block TV shows of certain ratings which they deem inappropriate for their children [7].

5.7 Market response to DRM

This section contains the market response to DRM in various products. This section will discuss and analyze how the market has responded to various products that have been introduced with DRM. The products mentioned in this section are those which were introduced in the last section. In addition, this section will also mention, but not analyze, other potential areas to research into.

DIVX was cancelled

From Circuit City's DIVX format, sales were very poor and forced Circuit City to eventually discontinue the format. One possible reason for this is that consumers may not have been willing to choose a format which had viewing restrictions on it while another, quite similar format did not have those restrictions. Other thoughts about consumer sentiments can be summarized as follows:

- While DIVX discs costed $4.49 each, and were cheaper than buying a DVD, they were more expensive than renting from a video store such as Blockbuster.
- Most DIVX movies only came in pan-and-scan formats and did not have any extras.
- Select retailers carried DIVX discs, Circuit City and its partners, and they were not open very late.
- Half of the major movie studios supported the DIVX format, while all movie studios supported DVD, meaning fewer titles were available for DIVX.

- DIVX was proprietary, meaning it was a defacto monopoly. Consumers may have been unsure that if DIVX were to dominate that the retailers selling DIVX would set prices without regards to competition.
- DIVX movies could be placed on moratorium by the movie company instantly. This means a movie company could disable the movies for whatever reason.

While DIVX media was cheaper than DVDs, viewing the content was restricted for the first 48 hours after inserted in the player. For any viewing after the initial 48 hour period, the player recorded this, and passed the information along to a billing center which billed accordingly. The DIVX format was released in time for the fall 1998 holiday season, but was discontinued on June 16th, 1999 due to high cost of introduction and limited public acceptance. This shows the DIVX format was not very well accepted, thus pulled from market after less than a year of availability [36].

Content Scrambling System cracked

Upon the release of DVDs, people realized there was no commercial support for DVD playback on computers which did not run Microsoft's Windows or Apple's Macintosh operating systems. Several groups of people on were quite upset that their particular systems were not allowed to play DVDs, because playback software required the approval of the DVD manufacturers. In 1999, Jon Lech Johansen reverse engineered the CSS algorithm and released a program called DeCSS, a program which was capable of decrying DVDs encrypted using CSS.

The response to CSS being cracked was quite large on the Internet. People on the Internet were waiting for a way to break the encryption for a few reasons, one being the ability to play DVDs on Linux. One response to CSS being broken, which is hard to argue how true it is, is that DVD sales increased as people were finally able to play them on any device with a DVD reader. Another response was the all of sudden availability of DVD copying software. This in turn probably led to more people purchasing DVD writers and DVD media, and arguably more sales of DVDs. From this, it seems if people are given the freedom to do what they want with the content, at least to view on hardware they desire, then everybody wins out as sales of DVDs increase.

An interesting note is, that under the DMCA, it is illegal to reverse engineer CSS for playback on Linux, under the illegal to reverse engineer for interoperability clause, but it is not illegal to play decrypted DVDs on Linux [4].

Sony Rootkit embarrassment for Sony Corporation

Regarding the Sony/BMG XCP Rootkit event of Fall 2005, it caused quite a bit of embarrassment for Sony/BMG Corporation. It was a public relations nightmare as people learned of the initial problem, learned the utility from Sony to fix the problem only made matters worse, and had lawsuits filed. Since the problem was discovered in the latter portion of 2005, it is difficult to tell if record sales for Sony/BMG in 2005 were affected by this. However, events such as this may have upset consumers, and possibly be part of the reason CD sales are dropping and stores using the Internet for distribution are doing well [32].

Librarians fearful of DRM

A recent BBC article stated that librarians in Britain are fearful of DRM. They dislike the idea of DRM since they are fearful of being digitally locked out of content by the people who control DRM. The librarians also said that DRM blocks out some of legitimate uses of the content. Britain's copyright law allows libraries to give access to, copy, and distribute items through a 'library clause' in the law's fair use section, but librarians are fearful that DRM will not allow them to use digital content in ways as they previously had used digital and analog content. Libraries are also fearful that content will not be accessible in the long term, for if the DRM key holder goes out of business or is hard to track down it would be next to impossible to use the content. In addition, the digital locks do not go away when the copyright period expires. So far, the libraries have voiced their concerns and formed a group called Libraries and Archives Copyright Alliance (LACA) to review DRM [76].

Video Game consoles been 'hacked/modded' to run bootlegged games

Video game console makers have had their own piracy concerns. In order to combat piracy of their video games, console makers have inserted their own forms of copy protection in videogames, such as different methods of preventing ripping the discs. As a result of this, modified or 'modded' consoles have appeared, mainly those with an additional chip to bypass or disable some of the locks built into the console. The success of game consoles has partly been due to the ease of 'modding' of a console.

Recently, however, console makers have expanded from their usual methods of copy protection by using newer schemes. For example, Sony Computer Entertainment America has released an authentication method called Dynamic Network Authentication System (DNAS). When games are played online, information about a user's hardware and software for authentication, copy protection, account blocking, game management, and other purposes. Games which are copied usually lack certain keys which are looked for by the DNAS, thus causing the server to disallow the user [1].

Flexplay not accepted

The next form of DRM that was commercially available and had not been embraced by consumers is FlexPlay. FlexPlay is a type of DVD where the data is stored on content that degrades over time, usually 48 hours. The technology was thought to pick up where formats such as DIVX failed. FlexPlay was launched in August 2003 but so far has generated little interest from movie studios, video rental companies, and consumers [51]. If this format is to become popular, one could imagine the amount of extra waste this would generate, as discs outside the 48 hour usage period would be useless and thrown away. Since only the portion of the disc which stores the content degrades over time, the remainder of the disc is useless, and this extra waste would cause even more junk to be thrown into our landfills. From this, the industry should have learned a second time that time limited content is not what the consumer wants. From this it is very clear that the consumer wants to be able to purchase media that does not have time restrictions, as they want to purchase it and not to worry about it.

GPLv3 forbids use of its code for copy protection uses

The next topic deals with a software license from the Free Software Foundation (FSF) version called the GNU General Public License (GPL). The latest version, version 3, is in its draft stages, and clauses have been included which state code licensed under the GPLv3 can not be used to produce anything that contains DRM. This is the response of the Free Software and Open Source Software (FOSS) community - a new software license that will prohibit the use of its licensed code for DRM related purposes. One thing to note it this license will only apply to code which is released under this license, and open source developers are free to stick with the older version, GPL v2.

One possible ramification of the use of GPLv3 is that tools which use DRM can not use open source as a base. For example, let us say the Linux Kernel was to migrate from GPLv2 to GPLv3. This would mean those versions of Linux would not be legally usable in devices which apply DRM. Devices such as Tivo, which use Linux, would not be able to use the Linux kernel, thus would either be forced to find a new operating system or to strip DRM from their product [55]. The migration to GPLv3 could potentially have a negative effect on corporations that use Linux in their products, as they would probably have to find another operating system to use. As of right now, there is not code released under the GPLv3, and as so, it may be tough to predict how the market will react.

Canadian record label pays for legal costs for one user against RIAA

In Canada, a major Canadian record company has hired a lawyer for a man accused of downloading music by the RIAA. The Nettwerk Music Group will pay for the defense of a man named in a suit filed in Texas. The CEO of the Nettwerk Music Group, Terry McBride, said "Suing music fans is not the solution; it's the problem" about the RIAA lawsuits. McBride, whose company represents artists such as Avril Lavigne, also said "Litigation is not artist development. Litigation is a deterrent to creativity and passion and it is hurting the business I love. The current actions of the RIAA are not in my artists' best interests." This shows this Canadian record label does not agree with the RIAA's method of lawsuits and feels unhappy by these actions [28].

Steam system from Valve

The Steam system used by Valve corporations has had its share of likes and dislikes by users. For many users, they are indifferent. Others are critical of Steam as Steam games require a user to log in and authenticate at least once before the game can ever be played. Others suspected Steam would migrate to a Pay-to-Play type of service, but the End User License Agreements (EULAs) of games do not state this, and altering the EULAs to allow this would be illegal. Another criticism of steam is the forced auto-updating of games, as the game is checked each time to see if it is up to date and an updated is forced if necessary [27].

eBooks

Electronic books are another place where DRM has been introduced. From their onset, publishers had been wary about eBooks without DRM as they could, in theory, allow making infinite copies of the media. Some forms of DRM restrict printing the content, others restrict the number of copies, and others restrict the particular hardware that can be used to view the content. Overall, eBooks have not caught on yet. Some people feel the cost of eBooks is not justified as having a paper copy of a book is worth more. Others feel eBooks should not be restricted in various ways, and others simply do not know eBooks exist.

In terms of sales, a total of 421,955 eBooks were sold in Q1 2004. The same period in 2003 saw 288,440 sales. Q1 2004 saw $3,233,220 in revenue compared to $2,516,469 in the same quarter 2003 [59]. Compared to book sales, these numbers look tiny, as book sales are in the hundreds of millions of dollars. Ebook sales are climbing, but not are not nearly at the levels which they were thought they would be at [5].

iTunes Store

The next example is the currently popular iTunes Store by Apple Computer. This system includes DRM in content that is purchased, but unlike other implementations of DRM, the restrictions are not nearly as tight. For example, while a song is tied to a particular computer, the owner can authorize up to 5 other computers that can access the content. In addition, Apple allows the music files to be burned to a CD. Apple Computer calls this their Fairplay DRM scheme, in otherwords, Apple allows using the content in manners which they deem fair [9]. Due to the vast success of the iTunes Store, it seems reasonable to think consumers feel the content is reasonably priced and the FairPlay DRM is reasonable. From this implementation of DRM, we see that consumers may embrace a service with DRM if the consumer feels the price of the content is reasonable and its restrictions are reasonable. Recently Apple has added movies and TV shows for sale on their iTunes Store. Disney movies, television shows, and music videos are also available from the iTunes Store. The video files are encapsulated in the same DRM as the music files are, Fairplay [8].

5.8 Business models using DRM

Next the author will examine some business models using DRM. Models which sell digital content will be summarized, as well as discussed for their practicality and success with consumers. From this, we can see if there are any important items for success in selling content with DRM, as well as use some ideas to propose a better distribution method in a further section.

iTunes Store

The business model of the iTunes Store is not very complex. Accessing it requires a computer, an Internet connection, and Apple's iTunes software. People can purchase individual music tracks for $0.99, or $9.99 per album, TV shows for $1.99 per episode, and movies ranging from $9.99 to $14.99. Since Apple was able to sign licensing agreements with the major labels to agree to using their service, and also publicized this quite well, their music store is a success. Even with this success, it seems as if Apple only makes a few cents per download, thus this model may not be lucrative by itself. However, Apple is probably making money on the combination of music and iPod sales, thus it can be called a successful model. Another thing to note is this content store may be driving sales in other areas, such as hardware. It is tough to draw direct correlation between the popularity of the iTunes Store and iPod and Apple Computer sales, but it would be tough to say the two are not related [43].

Old Napster, New Napster

The old Napster is what started the whole P2P revolution. The first version of Napster allowed anyone who connected to download any song any users had for no charge. The only cost of entry was a computer, an Internet connection, and obtaining the Napster software. After Napster became popular, it caught the eyes of the band Metallica and the RIAA, and eventually was shut down in 2001 by the RIAA. It was relaunched by Roxio Corporation in 2003 as a pay-per-download service.

The new version of Napster, Napster 2.0, has been online since October 2003 and has been selling songs, unlike the prior version which allowed downloads for free. However, it has not been as popular as iTunes, but has been able to sell some songs. Their new service works by paying a monthly fee to have access to songs, which can also be purchased. The purchased songs can be downloaded and placed on devices, but will become unusable if the subscription becomes terminated [33].

AllofMP3

Allofmp3.com is a music service from Russia where users pay for content based on volume of data downloaded, not per song. This differs from other services, such as Apple's iTunes because users do not pay per song. The music files can be downloaded in a variety of bit rates and compressed in a variety of codecs. All downloads are DRM free, meaning music can be shared among computers easily. The legality of this service is also disputed - the Russian Government says it is legal within Russia, but the legality in other countries, such as the US, is disputed [17]. To complicate the legality of this site even further, the World

Trade Organization has told Russia that this site could jeopardize Russia's entry into the WTO [17].

Cinemanow and World Cinema Online

CinemaNow and World Cinema Online are video distribution websites which use Microsoft's Windows Media Format to encode the video. Both companies allow the user to rent or purchase movies. World Cinema Online is geared more towards independent film makers, while CinemaNow carries movies from Hollywood. Consumers may not like CinemaNow due to its high price for movies, averaging $19, and some reviewers report the quality is noticeably less than DVDs [50].

Video on Demand

Video on demand (VOD) is a system where major cable providers allow users to select when they want to view content. It appears to be the next generation of the pay-per-view services offered by cable companies. It is bandwidth intensive, thus only major cable providers are able to offer this at present. VOD systems either download the content to a set top box or stream the content from the provider. The user is allowed to pause, rewind, and fastforward through the video. At the moment, the video can not be extracted from the set top boxes, thus the concern of stealing the content has not materialized yet.

Steam system from Valve

Steam was developed by Valve corporation to allow users to download, update, use content, and verify ownership of content. Initial versions of this system were very buggy, often not working at all. Initially it was used to make patching games easier, as it allowed the game to automatically update itself when it connected to the Internet instead of relying on the user to find the patch and manually update the game. Next it was used by Valve to activate games, starting with Half Life 2 in fall 2004. Valve requires purchasers of games to register with the Steam service before being able play the game for the first time. Steam next allowed the purchase of games via the Internet, where the game is downloaded from the Steam servers to the users' computer. Steam is also used to reduce the number of pirated copies of games by checking authenticity at each login. Additionally, Steam has logic to help reduce cheating in online games using the Steam service (Steam periodically scans memory to check for commonly used cheat programs). Since its introduction, Steam has not been the most stable nor most bug free. Steam has had problems periodically, such as the day Half-Life 2 was released the Steam servers were unreachable (possibly due to overloading). Other problems have been with pre-ordering with credit cards, SteamID reporting errors, and random periods of downtime. It is tough to say how well this model is doing; it is generating enough momentum that Valve has released games other than Half-Life 2 via steam, but it is a commonly griped about service among gamers [27].

Conclusions

From the above mentioned business models of distributing digital content, we see there is a successful model content distribution with DRM. We see the legality content distribution without DRM is questionable in the US, and while certain stores may be legal in other countries, their legality is disputed in the US. From the distribution methods listed, the Steam system appears to be a viable method for distributing software, although it is not without its problems. Cable companies with large, high speed networks are able to offer Video on Demand services to customers as they have the bandwidth required by such services. From the two legal music stores, we see the iTunes Store from Apple is more successful, as its restrictions more relaxed than its competitor's. In addition, the iTunes Store has the resources of Apple behind it, meaning iPod sales and marketing probably help drive sales. From this, we can conclude that digital content with DRM can be successfully sold, given the price is right and restrictions are reasonable to the consumer.

Chapter 6

Potentially Restrictive Technologies

This chapter will summarize different laws which have the potential to be restrictive in a manner analogous to DRM. Detailed discussion of the following are out of the scope of this paper, but these are other important areas to consider. The discussion will be limited to items which have not been discussed in this paper already.

Patriot Act

The USA PATRIOT ACT (Public Law 107-56) is short for "Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism" Act of 2001 and is a controversial piece of Federal legislation in the United States. It is aimed at helping government agencies find terrorists, but can also be viewed as a massive invasion of privacy. Some clauses of this law allow for wiretaps without obtaining a warrant, ability for government agencies to view library records, start of a foreign student monitoring program, etc. The powers given to the government could potentially infringe on the civil liberties of citizens within the US, even if they are not guilty of any crime.

Wire Tapping

Soon after the terrorist attacks on September 11, 2001, President Bush issued a secret order to the NSA to allow warrant-less wiretapping of people who may be suspected to be linked with Al-Qaeda and other terror cells. The NSA was found to have surveyed people, some of who were US citizens. This program was eventually ruled unconstitutional by the courts [58].

Limitations on exporting certain cryptographic related algorithms outside US

The USA has placed limits on exporting certain algorithms outside of the US. At the end of World War II, the US and its allies decided it may be militarily valuable to deny current and potential enemies access to cryptographic technology developed by the US and its allies. Regulations and export laws established that cryptography beyond a certain strength, strength being defined by the algorithm and key length, would not be licensed for export except on a case by case basis. The idea is not to make it so difficult for our agencies to decrypt other government's communications, especially those of our enemies using our own technology, while using the strong cryptographic algorithms for ourselves and making it tough for others to decrypt out messages [38].

Chapter 7

Conclusions

The goals of this paper are to describe what DRM is, to determine the purpose of DRM, to analyze what corporations think about DRM, and to analyze what effect DRM has on piracy. Additionally we describe the effect of DRM on the end user experience and explore the potential impact of DRM on societal norms. Observations of market response to products which contain DRM are analyzed to help determine consumer sentiment and lessons learned. Lastly we explore if DRM is a viable method for future content distribution and propose a successful business model for distributing copywritten material.

Have I explained to the reader what DRM is?

The reader is presented with a detailed overview of what DRM is in the background section of this paper. Some history behind DRM has also been presented. In addition, several past and present consumer products with various forms of DRM have been presented to the reader to help demonstrate how omnipresent DRM is.

What is the overall effect of DRM?

It is clear that DRM does not reduce piracy. In an attempt to reduce piracy, DRM introduces restrictions that consumers do not want. The desire to obtain content without the restrictions of DRM has caused piracy to increase. Some consumers do not feel their actions are in fact piracy, as shown in section 5.1.5. Consumers feel strongly that they should be able to do what they desire with content they have purchased. The DRM in content often hinders their usage, which they feel is allowed under the definition of "fair use", and thus some resort to piracy to remove the DRM.

The effect of DRM on the end user experience is that it limits the amount of freedom the user has with the purchased content. With DRM, fair use is limited to what the content authors and distributors feels is fair, preventing the user from being able to use the content in new, creative ways. For example, DRM in ebooks prevents the user from printing out parts of the book, forcing them to be tied to the device to read it, whereas paper books can be read anywhere.

The effect of DRM on society has the potential to hurt consumers, sales, and innovation. With DRM, fair use is restricted to what the corporations feel is fair use, and new businesses are not allowed to come up new methods for playing. For example, if DRM on CDs prevents them being ripped to computers, this would probably have hindered the industries that have grown due to music, such as online music stores, sales of portable devices, to some extent the purchase of high speed Internet connections by home users, and even some purchases of computers. The lack of tight restrictions allows users and corporations to experiment with content, developing new industries, and possibly forcing companies to become innovative in order to survive.

What are the corporations views on DRM?

Corporations feel the need to insert DRM into their products to protect their Intellectual Property (IP). Corporations feel the inclusion of DRM will reduce the number pirated copies of their content, while increasing their revenue as more users purchase their product. Additionally, corporations feel the user is obligated to purchase the content each time the format changes. For example, record companies want you to purchase CDs, then purchase the same content as MP3s, then purchase the same content as another format, etc, instead of converting the content from the CD to the format of your desire.

What affect does DRM have on piracy?

From the research performed for this paper, DRM does not seem to directly reduce piracy. It can be argued that it does the opposite, as consumers desire content that does not have the artificial locks and allows them the freedom to do what they desire. Due to the lack of evidence that DRM does in fact reduce piracy, it is impossible to say DRM definitively does reduce piracy. Since the purpose of DRM, as the corporations see it, is to reduce piracy, and there is no strong evidence showing DRM does in fact reduce piracy, it seems DRM is not achieving its goal. As DRM is not doing what it was designed for, it seems that DRM is unnecessary.

What is the impact of DRM on end user?

The effect of DRM on the end user is the end user has to accept DRM locks. Due to the inclusion of restrictions, the end user is not allowed to do what he wants with the content, even if it is legal under fair use, such as time shifting of content. He can only do what the content author feels is acceptable. Limiting what fair use is limits the creativity of end users, potentially stifling new business models for future content use. Additionally, there is currently no overseeing body to ensure the content creators do not abuse their power. Another observation is that people have been actively setting out to break the DRM encryption on almost all content, as people desire content which does not have restrictions and lets them do as they please and forgo the hassle introduced by the DRM locks.

How past DRM technology has been accepted by the market?

From the examples presented in this paper, the market seems to reject products with DRM that consumers feel is too restrictive. It appears that if a product is too restrictive to the consumer, the product will not sell. An interesting note is that usually a restrictive format loses to a similar format which is less restrictive. Additionally, products containing DRM that consumers feel is not too restrictive have ended up being accepted by the market, and consumers either find those restrictions acceptable or are not affected by those restrictions.

However, software products have not been rejected as often as hardware and other media formats containing DRM have been rejected. This is possibly due to the fact that companies who are selling software products have such great share of the market that the companies can use their position to force users to accept the DRM. DRM has been inserted slowly in software in such a way that consumers often do not realize the restrictions are present.

What are the possible ramifications of DRM?

Some possible ramifications of DRM are that new industries may be prevented from developing due to the restrictions. This in turn may hinder creativity and hurt society as innovation will be stifled and technology will stagnate. Additionally, social behaviors of people may be altered by the restrictions imposed by DRM.

Is there a viable model for content distribution at all?

From the business models presented which contain DRM, the iTunes Store business model seems to be the most successful. However, a DRM-free business model is preferred, as it would remove restrictions for the users. However, finding a good distribution method for DRM-free media which is legal, compensates the artists, is low cost, and accepted by the users is a difficult task. At the moment, it appears DRM can be used successfully in the content distribution area. An example of a very successful business model is the iTunes Store from Apple, as the iTunes Store has a significant share of the downloadable music and video markets.

Is there a distribution model that is fair?

Determining whether or not a distribution method is 'fair' is a tough task. What may be fair to one group, such as consumers, may seem unfair to other groups, such as media companies and artists. At the moment, is appears consumers find the iTunes Store model the most fair of the legal methods presented, as an overwhelming majority of digital music is purchased through the iTunes Store. However, the iTunes Store may be popular as a more 'fair' model may not be developed as of yet. One reasonable way to determine a 'fair' distribution method would be one where the consumers, the artists, and the media companies all vote on several different models and pick the one which makes the most groups happy, starting with the consumers, then the artists, and lastly the media companies. Additionally, periodic voting would be necessary in order to account for advances in technology and differing desires by all parties.

Is DRM predisposed to failure?

In some ways DRM is predisposed to failure. Technology which is restrictive and has an alternative which is similar with fewer restrictions will always have a difficult time being accepted, as consumers will most likely use the less restrictive one. However, some DRM seems to be acceptable, such as the case with Apple's Fairplay, but then again the Fairplay

DRM technology has been reverse engineered, so that may be why people are accepting it. In general, consumers like to have the freedom to do what they want with their purchased media.

7.1 One possible view of DRM in the year 2050

I predict that the corporations will include DRM in future products, slowly increasing the restrictions until the consumers one day realize the restrictions are far too strict and reject DRM. Consumers will be fed up with being told what to do by the corporations, will want to regain control of their purchased content, and form a new group to distribute content directly from the artists to consumers. This will cause the current business model to erode, and the current corporations will be forced to adapt to the new means of distribution or lose market share. I predict DRM will lead to the extinction of the RIAA, which will be too slow to adapt to changes in the digital age, and the replacement will be a distribution method which is run by the artists and consumers.

Currently, there are many forces at work to dictate exactly what will happen. If the RIAA becomes too restrictive, then companies that make hardware to play music may start to suffer as hardware sales would drop as nobody would be able to use the devices. In response to lackluster sales, and in an effort to get more sales, another company could be innovative and offer music in a form which has fewer or no restrictions built into it. Alternatively, hardware makers may provide devices with loopholes to get around the restrictions. If consumers feel this alternative is better, then it will become popular, and the innovative corporation will become the dominant player in the content distribution industry while the older method starts to suffer. The key thing to remember is that all companies involved are out to make money, and if one starts to suffer, it will either die out or be forced to innovate and introduce a better alternative.

Another thing to keep in mind is that consumers may not purchase content if the restrictions are too strict, as seen by some examples of failed technologies. Currently, the strategy of the industry seems to be to slowly introduce the restrictions, and who knows what they intend to do in the future. It is worth noting that if consumers feel the restrictions are too strict that they will reject the technology and not purchase the content. This in turn will hurt the companies selling the products, as consumers voting with their wallets will hurt corporations bottom lines, and thus force the corporations to try again and release something which is less restrictive.

Future content distribution method

As the current business models for content distribution may not be perfect, the author has put thought into a potentially improved distribution method. I propose a possible future content distribution method consisting of an online store with the following characteristics. The online media will be available through a central store at a reasonable price which will be decided upon by the artists. Consumers will be allowed to vote whether or not the content appears to be fairly priced, as well as the quality of the content and their overall satisfaction. The online media store should be run by a group of people voted upon by the artists and the consumers to act fairly in everybody's interests, and periodic voting will occur to ensure the artists and consumers are happy with the leadership. Additionally, the store will try to find a middle ground on price, quality, and other services where the consumers and the artists are both happy.

The media will be sold directly by the artists, eliminating the middle man. Content distribution via the Internet will be aided with the help of a distributed downloading protocol, perhaps a modified version of the BitTorrent protocol. The BitTorrent protocol breaks down large files into small chunks, usually 256kB or 512kB. People who upload these small chunks are called seeders, and people who download these are called peers. Peers download the fragments in any order from various sources, and in the end when all chunks are downloaded, the file transfer is complete. The protocol is 'smart' enough to choose the peer with the best network connections for the fragments that it is requesting. One way BitTorrent increases overall efficiency is to request chunks from seeders that are the most rare, making most fragments available widely across many machines and hopefully avoiding bottlenecks. A content distribution scheme centered around BitTorrent may ease the problems of bandwidth and distribution from a central server.

In addition to distribution via the Internet, hard copies of the media should be available for people who do not have computer or Internet access. A mail order store would be appropriate as it would remain under the control of the group appointed by the artists and consumers to run the online media store. However, establishment of Brick and Mortar stores could happen if consumers and artists agree on a method of running the stores.

This new group would understand the dangers of DRM, thus forbid any artificial locks on the content and allow the consumer to do what they please with the content. The content will be open to all, which means piracy will be unavoidable, but the hope is consumers will be on their honor to pay for content.

From this report, we see that corporations feel DRM is a major part of digital content as it allows the corporation to enforce policies which will protect their Intellectual Property. This paper has shown that DRM does not directly reduce piracy, but instead has a tendency to increase piracy as consumers desire content without digital restrictions. This finding, as well as general awareness about DRM is important as it will affect everyone in the near future.

Bibliography

[1] Sony Computer Entertainment America, *DNAS*, http://www.us.playstation.com/DNAS, Retrieved on March 2006.

[2] Jose Avila, *FedEx box furniture photographs & information*, http://www.fedexaminer.com/FedEx/modules.php?name=FedExFurniture, Retrieved on March 2006.

[3] Ken Barnes, *Album sales slump as downloads rise*, http://www.usatoday.com/life/music/news/2006-01-04-music-sales-main_x.htm, Retrieved on January 2006.

[4] Jeffrey A. Bloom, Ingemar J. Cox, Ton Kalker, Jean-Paul M. G. Linnartz, Matthew L. Miller, and C. Brendan S. Traw, *Copy protection for DVD video*, Proceedings of the IEEE **87** (1999), no. 7, 1267–1276.

[5] Edward Christman, *2005 numbers crunched: A strong book year - better - performing releases than in '04*, http://www.thebookstandard.com/bookstandard/news/retail/article_display.jsp?vnu_content_id=1001808409, Retrieved on January 2006.

[6] Philippe Ciaravola, *Impact of computers on society*, Course: Computer Science - COMP 102, McGill University, staff.cs.mcgill.ca/vola/cs102/, December 2005.

[7] Federal Communications Commission, *FCC v-chip*, http://www.fcc.gov/vchip/, Retrieved on March 2006.

[8] Apple Computer Corporation, *Apple - iTunes - iTunes overview*, http://www.apple.com/F/overview/, Retrieved on November 2006.

[9] ______, *Apple - support - iTunes store - authorization FAQ*, http://www.apple.com/support/itunes/musicstore/authorization/, Retrieved on November 2006.

[10] Macromedia Corporation, *Product activation*, http://www.macromedia.com/software/activation/version2/faq/, Retrieved on March 2006.

[11] Microsoft Corporation, *Windows XP product activation*, http://www.microsoft.com/windowsxp/evaluation/features/activation.mspx, Retrieved on August 2002.

[12] ———, *Microsoft security glossary*, http://www.microsoft.com/security/glossary.mspx#digital_rights_management, Retrieved on December 2005.

[13] ———, *Windows media DRM FAQ*, http://www.microsoft.com/windows/windowsmedia/forpros/drm/faq.aspx, Retrieved on October 2005.

[14] ———, *Microsoft product activation: FAQ - software piracy protection*, http://www.microsoft.com/piracy/activation_faq.mspx, Retrieved on March 2006.

[15] ———, *Volume licensing home page*, http://www.microsoft.com/licensing/default.mspx, Retrieved on April 2006.

[16] United States Supreme Court, *SONY CORP. v. UNIVERSAL CITY STUDIOS, INC., 464 U.S. 417 (1984)*, Argued January 18, 1983 Reargued October 3, 1983 Decided January 17, 1984.

[17] Thomas Crampton, *Russian download site is popular and possibly illegal*, http://www.nytimes.com/2006/06/01/world/europe/01cnd-mp3.html?ex1=1306814400&en=4c9bcba30952e86b&ei=5090&partner=rssuserland&emc=rss, Retrieved on June 2006.

[18] Cory Doctorow, *Why some "piracy" can increase overall revenues*, http://www.boingboing.net/2005/08/24/why_some_piracy_can_.html, Retrieved on August 2005.

[19] Cory Doctrow, *The 3-minute guide to the broadcast flag: A brief overview explaining what it is and why you should care*, http://www.eff.org/broadcastflag/three_minute_guide.php, Retrieved on March 2006.

[20] EContent, *Econtentmag.com; why aren't ebooks more successful?*, http://www.econtentmag.com/Articles/ArticleReader.aspx?ArticleID=18144&ContextSubtypeID=11, Retrieved on October 2006.

[21] The UCLA Online Institute for Cyberspace Law and Policy, *The Digital Millenium Copyright Act - overview*, http://www.gseis.ucla.edu/iclp/dmca1.htm, Retrieved on March 2006.

[22] Electronic Frontier Foundation, *Electronic Frontier Foundation*, http://www.eff.org/IP/broadcastflag/, Retrieved on March 2006.

[23] ———, *MPAA (motion picture association of america) dvd cases archive*, http://www.eff.org/IP/Video/MPAA_DVD_cases/, Retrieved on April 2006.

[24] ———, *Unintended consequences: Seven years under the DMCA*, http://www.eff.org/IP/DMCA/unintended_consequences.php, Retrieved on April 2006.

[25] Free Software Foundation, *GNU General Public License*, Free Software Foundation, third, second draft ed., 2006.

[26] Bryan Gardiner, *MPAA: Frustrated consumers will pirate*, http://www.pcmag.com/article2/0,1895,2031751,00.asp, Retrieved on October 2006.

[27] Garmer, *Valves tracker*, http://www.cs-extreme.net/features/tracker/tracker.asp, Retrieved on March 2006.

[28] Antone Gonsalves, *Record label supports man accused of sharing music illegally*, http://www.informationweek.com/security/showArticle.jhtml?articleID=177104855, Retrieved on January 2006.

[29] Trusted Computing Group, *Trusted Computing Group website*, https://www.trustedcomputinggroup.org/, Retrieved on March 2006.

[30] Universal Music Group, *Universal Music Group and RealNetworks form strategic alliance*, http://www.umusic.com/static/press/01072000.htm, Retrieved on January 2000.

[31] Bill Hagen and Marsha Longshore, *IEEE to revise new copyright form to address author concerns*, http://www.ieee.org/portal/pages/newsinfo/dmca.html, Retrieved on April 2002.

[32] Arik Hesseldahl, *Spitzer gets on Sony BMG's case*, http://www.businessweek.com/technology/content/nov2005/tc20051128_573560.htm, Retrieved on November 2005.

[33] ______, *A needy Napster searches for takers*, http://www.businessweek.com/technology/content/sep2006/tc20060919_053475.htm, Retrieved on September 2006.

[34] HowStuffWorks.com, *How Flexplay works*, http://www.flexplay.com/how-flexplay-works.htm, Retrieved on March 2006.

[35] Dow Jones/AP, *Sony BMG settles cd case*, http://www.nytimes.com/2006/05/23/business/media/23sony.html?ex=1306036800&en =b87f7a06d9d88a45&ei=5088&partner=rssnyt&emc=rss, Retrieved on May 2006.

[36] The DVD Journal, *What was divx?*, http://www.dvdjournal.com/extra/divx.html, Retrieved on March 2006.

[37] Gregg Keizer, *NY AG blasts Sony, says rootkit cds still for sale*, http://www.techweb.com/wire/ebiz/174402972, Retrieved on November 2005.

[38] Fred Von Lohmann and Wendy Seltzer, *Death by DMCA*, Spectrum **1** (2006), 1.

[39] Christopher May, *Digital rights management and the breakdown of social norms*, http://outreach.lib.uic.edu/www/issues/issue8_11/may/index.html, Retrieved on October 2003.

[40] Declan McCullagh, *Lexmark invokes DMCA in toner suit*, http://news.com.com/2100-1023-979791.html, Retrieved on January 2003.

[41] Stanley Milgram, *Obedience to authority: An experimental view*, Harpercollins, 1974.

[42] Nielsen NetRatings, *Fifty million internet users connect via broadband, rising 27 percent during the last six months, according to nielsen//netratings*, http://www.nielsen-netratings.com/pr/pr_040108_us.pdf, Retrieved on January 2004.

[43] News.com, *iTunes outsells traditional music stores — CNET news.com*, http://news.com.com/iTunes+outsells+traditional+music+stores/2100-1027_3-5965314.html, Retrieved on November 2005.

[44] Motion Picture Association of America, *Fighting movie piracy*, http://www.mpaa.org/piracy_FightPir.asp, Retrieved on April 2006.

[45] ______, *What is internet piracy?*, http://www.mpaa.org/piracy_internet.asp, Retrieved on April 2006.

[46] ______, *Who piracy hurts*, http://www.mpaa.org/piracy_Consumers.asp, Retrieved on March 2006.

[47] Recording Industry Association of America, *Recording Industry Association of America*, http://www.riaa.com/issues/piracy/default.asp, http://www.riaa.com/issues/piracy/riaa.asp, Retrieved on March 2006.

[48] Kathleen O'Toole, *The Stanford prison experiment: Still powerful after all these years (1/97)*, http://stanford.edu/dept/news/relaged/970108prisonexp.html, Retrieved on January 1997.

[49] United States Patent and Trademark Office, *Glossary*, http://www.uspto.gov/main/glossary/, Retrieved on March 2006.

[50] Robert Pegoraro, *Movielink and CinemaNow: Hardly worth the effort*, http://www.washingtonpost.com/wp-dyn/content/article/2006/05/13/AR2006051300187.html, Retrieved on May 2006.

[51] Associated Press, *Hurry up and watch: DVDs time out*, http://www.wired.com/news/digiwood/0,1412,65707,00.html, Retrieved on November 2004.

[52] Robert J. Sales, *MIT responds to RIAA subpoena*, http://web.mit.edu/newsoffice/2003/riaa.html, Retrieved on July 2003.

[53] Bruce Schneier, *Real story of the rogue rootkit*, http://www.wired.com/news/privacy/0,1848,69601,00.html, Retrieved on November 2005.

[54] Seth Schoen, *Trusted computing: Promise and risk*, http://www.eff.org/Infrastructure/trusted_computing/20031001_tc.php, Retrieved on March 2006.

[55] Peter Seebach, *Linux on board: Blowing the lid off of tivo*, http://www-128.ibm.com/developerworks/linux/library/l-lobtivo/, Retrieved on July 2005.

[56] ———, *Standards and specs: Digital rights management: When a standard isn't*, http://www-128.ibm.com/developerworks/power/library/pa-spec11/?ca=dgrlnxw06, Retrieved on November 2005.

[57] Wendy Seltzer, *Waving flags of victory*, http://www.eff.org/deeplinks/archives/003555.php, Retrieved on May 2005.

[58] Ryan Singel, *Judge halts NSA snooping*, http://www.wired.com/news/politics/0,71610-0.html?tw=wn_index_3, Retrieved on August 2006.

[59] Macworld Staff, *ebook sales rocket*, http://www.macworld.co.uk/news/index.cfm?NewsID=8848&Page=1&pagePos=11, Retrieved on June 2004.

[60] NewsForge Staff, *GPLv3 draft analysis*, http://software.newsforge.com/article.pl?sid=06/01/17/1454213, Retrieved on January 2006.

[61] Howard Stringer, *The future of TV - U.K.*, http://www.sony.com/SCA/speeches/041118_stringer.shtml, Retrieved on November 2004.

[62] Wikipedia the free encyclopedia, *Broadcast flag*, http://en.wikipedia.org/wiki/Broadcast_flag, Retrieved on March 2006.

[63] ———, *Bsd licence*, http://en.wikipedia.org/wiki/BSD_license, Retrieved on March 2006.

[64] ———, *DeCSS*, http://en.wikipedia.org/wiki/DeCSS, Retrieved on March 2006.

[65] ———, *Digital Millenium Copyright Act*, http://en.wikipedia.org/wiki/DMCA, Retrieved on March 2006.

[66] ———, *Digital rights management*, http://en.wikipedia.org/wiki/Digital_Rights_Management, Retrieved on March 2006.

[67] ———, *DVD region code*, http://en.wikipedia.org/wiki/DVD_region_code, Retrieved on March 2006.

[68] ———, *ebook*, http://en.wikipedia.org/wiki/Ebook, Retrieved on March 2006.

[69] ———, *High-bandwidth digital content protection*, http://en.wikipedia.org/wiki/HDCP, Retrieved on March 2006.

[70] ———, *User operation prohibition*, http://en.wikipedia.org/wiki/User_operation_prohibition, Retrieved on March 2006.

[71] Benjamin R. Thompson, *Personal interview*, 20 February 2006.

[72] Fred von Lohmann, *Fair use and digital rights management*, http://www.eff.org/IP/DRM/fair_use_and_drm.html, Retrieved on April 2002.

[73] ———, *FairPlay: Another anticompetitive use of DRM*, http://www.eff.org/deeplinks/archives/001557.php, Retrieved on May 2004.

[74] ———, *Are you infected by Sony-BMG's rootkit?*, http://www.eff.org/deeplinks/archives/004144.php, Retrieved on November 2005.

[75] J. Wynia, *PDF DRM, why ebooks haven't "taken off" and how I wasted $150 in time on a $9 ebook*, http://www.wynia.org/wordpress/2005/10/29/pdf-drm-why-ebooks-havent-taken-off-and-how-i-wasted-150-in-time-on-a-9-ebook/, Retrieved on October 2005.

[76] Ian Youngs, *Libraries fear digital lockdown*, http://news.bbc.co.uk/2/hi/technology/4675280.stm, Retrieved on February 2006.