Global Information Assurance Certification Paper

Shawn Hayden
GSEC Practical v1.4 Option 1
June 26, 2002

PKI and Smart Card Solution for Preventing Illegal DVD Copying (Piracy), while Protecting the Rights of the Copyright Owner and the Consumer

ABSTRACT

This paper looks at several angles concerning DVD copying: the views of copyright owners, consumers and pirates; copyright laws; and copyright court cases. It also provides a solution, which protects the rights of both the copyright owner and the consumer, and prevents the pirating of copyrighted works.

This PKI Smart Card based solution allows consumers to make backup copies of their legally owned DVDs, and at the same time protecting the copyright owner's rights and prevents piracy.

INTRODUCTION

I have a small personal library, a collection, of music Compact Disks (CDs) and movie Digital Versatile Discs (DVDs) legally purchased from a retailer. There are some CDs and DVDs that my family really enjoy and use more often than others. As most people know, the more you use such media, the more it is exposed to damages (heat, scratches, and such), thereby reducing the operation and lifetime of the media. For instance, I have several music CDs that have been destroyed by deep scratches.

I also purchased a copy of *Titanic* Wide Screen DVD and managed to scratch it severely. Questions came racing into my mind, of whether or not it is legal to make a copy of this Movie? Is it legal, since I now own a thrashed DVD version of *Titanic*, to borrow a friend's *Titanic* DVD, or to rent the DVD to make a backup copy? Also, questions like, "When I bought *Titanic*, did I just buy the DVD plastic media, so when it is unreadable by the player, am I out of luck, or did I buy the movie, the contents on the plastic media, presented in a DVD format?"

When you purchase a DVD or CD, you are interested in the works contained on the plastic media versus the media itself. You watch a movie to see the movie, not to see the DVD media. Therefore, it seems as if you should be able to make a legal copy/backup of this movie, since you have purchased one legal copy of the work on DVD media. Possibly, you should also be able to keep the original copy of the work sacred and store it in a safe place, and then use the backup copy of the same work for personal use only, so as to not ruin the original media containing the work you purchased. By using the original work, you subject the

media to wear and tear. As an owner of one copy of this movie, you may want to keep the integrity of the movie without worrying about the physical media or format involved.

The plastic CD itself is just the medium and format in which the copyright owner has transferred their copyright work to you, the consumer, under the conditions of copyright law and its license for your personal use. Also, if I did purchase the movie, then it seems I should be able to legally own a backup copy of this movie on any media and format that I choose.

DVDs are encrypted to prevent illegal access and unauthorized copying of the copyrighted work. Decrypting the DVD has several advantages and disadvantages. Consumers can make a backup of their DVD and/or they can play their DVD on a Linux Box. For pirates, it makes it easier to make copies and distribute them. The following quote briefly explains the CSS encryption and the utility DeCSS.

> "CSS is an encryption-based security and authentication system that requires use of 'appropriately configured hardware,' such as a DVD player or a computer DVD drive, to decrypt, unscramble, and play back--but not copy--motion pictures on DVDs. CSS has been licensed to hundreds of DVD player manufacturers and DVD content distributors in the U.S. and around the world. In October 1999, only three years after its introduction into the consumer electronics market, a Norwegian teenager allegedly hacked CSS and began offering, via the Internet, a software utility called DeCSS that enables users to break the CSS copy protection system and hence to make and distribute digital copies of disembodied VOB files from DVD movies via their PC hard drives. Designed to enable Linux users to play back DVDs via their DVD-ROM drives in the absence of a licensed software DVD player for Linux, the DeCSS hack sent Hollywood into paroxysms of terror since it signaled the fallibility of the control measures it had imposed to date." (Block)

The misuse of copyrighted works by people is illegal. When people misuse something, it does not mean the rights and laws protecting good consumers should be taken away. If somebody runs over another person, should the law change to prevent all people from driving automobiles? No, the person who has broken the law, by definition, if the law is constitutional, has done something wrong and should be prosecuted by the law with justice being done.

The primary theme running through most of my questions deal with the digital copyright law. These questions about DVD media and digital copyright law led me to do some research and establish a few main questions to answer. With my preconceived ideas of what I think is legal, I will venture to find answers to the questions that I asked and determine whether I can legally decrypt my DVD and make a backup copy.

So, we will look at the views of copyright owners, consumers and pirates; copyright laws; copyright court cases; and a PKI smart card solution that protects the rights of both the copyright owner and the consumer, and prevents the pirating of copyrighted works, even when DVDs are backed up.

VIEWS OF COPYRIGHT OWNERS, CONSUMERS, AND PIRATES

Ethically, people should benefit and have their rights concerning their intellectual property protected by law. If people cannot make a profit from their works, chances are they are not going to be able to produce new and possibly groundbreaking materials for consumers to enjoy and benefit from. Yet, from the consumer's viewpoint, we should be able to use and protect both the work and media for our personal use, while respecting the copyright owners rights. From a pirate's perspective, he cares little about laws concerning copyright works.

Now, lets look further at some needs of both the copyright owner and consumer that should be addressed to help understand their view points and rights. These aren't the complete, entire viewpoints, but they do address some major questions about copyright protection and consumer rights.

Copyright owners Standpoint:

First, let's put ourselves into the shoes of a copyright owner and ask some honest questions. Let's see what is important to us concerning the works that we produce for out livelihood.

1) If we created a copyrighted work, as the owner of that work, should we expect to legally profit from its production, distribution, and exhibition? Of course, this work belongs to us. If we could not profit from the work, we might not share it or create other new works. As the owner of the work, we want to make a living from our labors in creating these works.

2) Would we be angry, or consider it illegal, if others pirated our copyrighted material for their personal gain? Of course, when people use or copy something that they have not purchased, they are pirating our copyrighted work. They are stealing our livelihood and, under copyright legislation, these actions are illegal.

3) On the other hand, as copyright owners, would we be angry, or consider it illegal, if someone, a consumer, made legal copies to archive/backup our copyrighted works that they purchased legally? Probably not. If the archive is used only for the consumer's personal use. After all, plastic, digital and paper media does not last forever. When we sold them our copyrighted work, we were selling the works and not necessarily the media. We would only consider the copying illegal if they used the copies to pirate our works.

4) Would we be mad, or consider it illegal, if they actively used their personal archive/backup to simplify the management of their library and archive the original copyrighted work? Probably not. It is much easier for the consumer of copyrighted material to actively use his archived library to obtain access to our works. The consumer can easily manage and use all of their purchased copyrighted material in one place. The consumer can store his original media to prevent its damage.

Consumers Standpoint:

Now, as the consumer who purchases copyrighted material for the purpose of personal use, let's ask some questions.

1) Should I be able to make a legal copy of copyrighted material I purchased to prevent its damage and protect my investment? Yes, a consumer has a right to protect his purchases and investments.

2) If I can make a copy, how do I do that today? Well, there is no legal way to make a backup copy of a DVD. There is software that you can use, but it first decrypts the copyright protection encryption on the DVD, and is illegal under current laws.

3) Should my rights of "fair use" be eliminated because of piracy? No, my rights should also be protected and not taken away because of others pirating copyrighted materials.

4) What can I, the consumer, do to prevent piracy? By not taking part in illegal acts of piracy, such as distributing copies of material that does not belong to you or others. Keep material for your own personal use. If you can't afford something, then wait until you can.

Pirates Standpoint:

Obviously, the standpoint of the pirate is not a justifiable issue in this paper. By definition, the pirate is a thief, and he will steal the works, and the money of a copyright owner, and will reduce the future markets for both consumer and the owner.

Is there ever a justification for stealing the copyrights from another person? No, there is never a time when you are justified for stealing another's copyrighted works. People can survive without watching or listening to digital media.

COPYRIGHT LAW OF THE UNITED STATES: COPYING A DVD

Have you ever taken time to read the warnings on DVD movies when they first start up? Here are the warning displayed at the beginning of a George Lucas DVD movie, "*Star Wars: Phantom Menance*":

> "FBI WARNING – Any use or exhibition of this video other than non-commercial home viewing is prohibited. Federal law provides severe civil and criminal penalties for the unauthorized reproduction, distribution, or exhibition of copyrighted motion pictures, videotapes or video discs. Criminal copyright infringement is investigated by the FBI and may constitute a felony with a maximum penalty of up to five years in prison and/or a $25,000 fine."
>
> "ATTENTION – International agreement and national law protect copyrighted motion pictures, video tapes and sound recordings. UNATHORIZED REPRODUCTION, EXHIBITION OR DISTRIBUTION OF COPYRIGHTED MOTION PICTURES CAN RESULT IN SEVERE CRIMINAL AND CIVIL PENATLITIES UNDER THE LAWS OF YOUR COUNTRY. The International Criminal Police Organization – INTERPOL has expressed its concern about motion picture and sound recording piracy to all of its member nation police forces (Resolution adopted at INTERPOL General Assembly, Stockholm, Sweden, September 8, 1977.)"

Breaking the copyright law can have some severe penalties according to these warnings. When dealing with issues of legality, one must first reference the law under which they are held accountable. What do the current copyright laws and previous court cases say about copying encrypted DVDs?

The Copyright Law of the United States is found in Title 17 of the U.S. Code. The Digital Millennium Copyright Act (DMCA) was signed by the U.S. Congress in 1998, which amended Article 17 of the United States Code, to incorporate many of the copyright laws found in the World Intellectual Property Organization Treaty of 1996 (WIPO).

The DMCA added laws to protect the copyright owner by preventing the piracy of their copyrighted works. "Key among the topics included in the DMCA are provisions concerning the circumvention of copyright protection systems, fair use in a digital environment" (Filzen).

According to the DMCA, Sec. 1201 (a)(2), "No person shall manufacture, import, offer to the public, provide, or otherwise traffic in any technology, product, service, device, component, or part thereof, that— (A) is primarily designed or produced for the purpose of circumventing a technological measure that effectively controls access to a work protected under this title." Also, under (3)(a), "to 'circumvent a technological measure' means to descramble a

scrambled work, to decrypt an encrypted work, or otherwise to avoid, bypass, remove, deactivate, or impair a technological measure, without the authority of the copyright owner."

The following statement sums up the ideal relationship between copyright law and "fair use":

> "Think of it this way: Copyright law -- which says you can't say or publish certain things under certain circumstances -- does seem to run afoul of say-and-publish-anything-you-want Free Speech rights. The way out of this seeming impasse happened when US courts invented, and Congress seconded, the concept of "fair use" -- which balances copyright protection with free speech rights. (McCullagh)

On Wirednews.com, in the article entitled "Tuning up Digital Copyright Law," Brad King sums up the war between protecting the rights of the copyright owner under the DMCA and the "fair use" of the consumer.

> "'Large media corporations have purchased a law from Congress and that has upset the balance between copyright holders and users,' Marti said. 'There is a major movement from the studios to prevent the distribution of legitimate software programs that came simply out of the reverse-engineering of an application.'
>
> Taylor said breaking encryption and posting the pirate-friendly utilities is equal to making a key of somebody else's locks, then going out and giving away copies of the keys and directions to the locks.
>
> 'If you don't get a chance to control what happens to the content you create, then you're not going to fulfill the full potential of the Internet because people are afraid of losing their intellectual property,' Taylor said.
>
> But Marti said the motion picture association is asking for too much control.
>
> 'Look at the people that have been called in the DeCSS trial, all the motions filed and all of the evidence presented. They haven't used one frame of pirated movies,' Marti said. 'This is about anti-circumvention, reverse engineering, and fair use. The DMCA is about the large copyright holders exercising unprecedented control over how you use a product once you've legally purchased it."

Piracy is a major concern in the movie industry, and rightly so. They have a lot to lose. The media industry wants to "control" and prevent the pirating of their works. This is an understandable concern; however, the rights of the consumer also have to be thought of and protected.

Copying CDs to one's personal music archive is very easy using Windows Media Player. Windows Media Player, by default, encodes your CD tracks into WMA files, which compresses them to a very small file size, and rips (copies) them to your hard drive. You can rip a 70-minute (650 MB) music CD into 60 MB with near CD quality in a matter of minutes. I can legally backup and archive my entire personal CD library in one place. There is no encryption on music CDs; therefore I have not violated the DMCA.

However, the DMCA states a person cannot decrypt the encryption on technology, CSS, which protects the copyright on the DVD. Next, we discuss a couple of court cases dealing with the DMCA.

COPYRIGHT COURT CASES: DMCA and Encryption

According to current copyright law, there is no permission given to consumers to decrypt their DVD, which prevents them from also making a backup copy. The DMCA "Outlaws the manufacture, sale, or distribution of code-cracking devices used to illegally copy software." Two court cases deal strictly with the DMCA and DVD encryption.

Case 1: Universal City Studios vs. Shawn C. Reimerdes (2002)

This court case found that under the DMCA, a utility called DeCSS, which decrypted the CSS encryption on a DVD, is illegal. DeCSS is several lines of code that decrypts a DVD and allows a user to copy the DVD. Even if a user has the right to copy a DVD, the software to decrypt it has been found illegal, thus preventing the copying of the DVD. This case directly supports the copyright owners and lacks any consideration for the "fair use" protection of the consumer.

Case 2: 321 Studios vs. MGM; Tri-Star; Columbia; Sony; Time Warner; Disney; Universal City Studios; The Saul Zaentz Co.; and PIXAR (2002)

The second case is where 321 Studios, who create DVD COPY PLUS software is suing the movie industry to allow its software to be used by consumers to backup their DVDs. This software is packaged and has several labels warning against violation of copyright laws. This software also has to decrypt the DVD before being able to copy its contents to the hard drive.

However, on DVDs, you cannot copy them without first decrypting the encryption algorithm which is put on their to prevent piracy. This prevention mechanism to stop piracy affects the consumer's "free use". Copying of any copyrighted work as a backup should be legal for personal use only under "free use."

Since, the major concern of copying DVDs in the copyright legislation is to prevent piracy, we should craft a solution with this in mind, and also the rights of copyright owners and consumers.

SOLUTION

The solution needs to be threefold. It needs to protect the rights of copyright owners and consumers, while preventing piracy. A solution that takes away either the rights of the copyright owner or the consumer in the hopes of preventing piracy is not adequate. It needs to protect both parties' rights.

The DMCA protects the copyright owner but not the consumer. It does not allow for the consumer to protect his investment when the media has *control-access copyright protection* type of encryption. Therefore this is not an adequate solution, since it limits the consumers "free use."

Several other solutions include adding watermarks or increasing the encryption, but none of these solutions address the issues of consumer "fair use." All these solutions simply make it harder to copy a DVD, and thus are still taking away the rights of the consumer.

We need a solution that makes it hard to illegally copy a DVD and at the same time, protect the rights of the copyright owner and the consumer.

PKI and Smart Cards

This idea for a smart card solution comes from a 1998 proposal by NDS for "IFE DVD Security." They recommended several smart card solutions, such as the incorporation of a smart card reader in the DVD player and the use of keys.

Smart cards (SC) along and a public key infrastructure (PKI) complement each other very well.

There are two types of encryption keys, symmetric and asymmetric. A *symmetric* key uses the same key to encrypt and decrypt data. Decrypting and encrypting is much faster with symmetric keys. *Asymmetric* keys use two keys. Each key can only decrypt that which the other key encrypts.

In PKI, the two keys are given names, the private key and the public key. As the names sound, everyone knows the public key. The private individual is the only one holding the private key, and is this private key must be kept secure. Different secure stores can be used, but one such secure store is a smart card, which I recommend to store the private key. So, when something is encrypted with the public key, only the private key can decrypt, and vice versa. (Hardie).

So, the use of PKI and smart cards can solve the three issues that have to be addressed. Herein, I only discuss the process for using PKI and smart cards. The technology has been developed, but it needs to be implemented.

Process for Encrypting DVDs

1) A pair of PKI keys must be created: a Public Key (PubK1), and a Private Key (PrivK1). Also, a Symmetric Key (SK1) is created.

2) The movie is encrypted with SK1. SK1 is symmetric and is the only key that can decrypt the movie.

3) SK1 is then encrypted with PubK1. Remember, only the Private Key, PrivK1, can decrypt the Public Key, PubK1.

4) The movie and the encrypted SK1 is stored on the DVD. This DVD is now referred to as the PKI Protected DVD (PP-DVD).

5) PrivK1 is stored on a SC.

Only PrivK1 can decrypt PubK1. In step 3, we encrypted SK1, with PubK1, therefore we can only decrypt SK1 with PrivK1. Now we have SK1 to decrypt the PP-DVD. After inserting the PP-DVD and the SC with the correct private key, the process for decrypting the PP-DVD starts and can be seen in Figure 1.

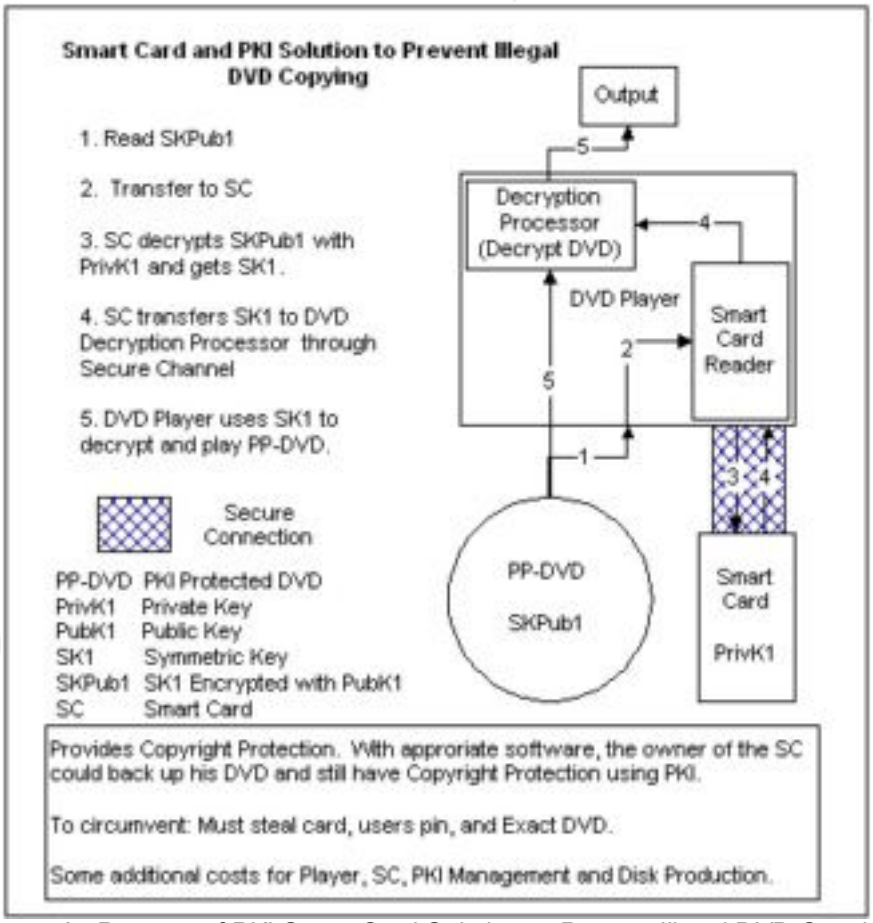

Figure 1: Process of PKI Smart Card Solution to Prevent Illegal DVD Copying.

Pros

- This PP-DVD is a long-term solution and can be used for different digital media.
- Copyright owner protection - The PKI encryption ensures that only the holder of the SC with correct private key can decrypt the movie.
- Consumer protection - Standard PP-DVD copy/backup software could be developed by someone, perhaps the movie industry, which would allow users to backup their PP-DVD to another format (compressed) and encrypt the copy using the same keys. This software could also include a PP-DVD software player that would utilize these encrypted backed up copies. Again, since the copy is encrypted using the PKI keys of the original, the copyright owner protection is still insured.
- Piracy - Prevented due to the fact that hacking a symmetric key for every PP-DVD made would be nearly impossible. The only way to find the symmetric key is by brute force, trying every possible combination.
- Scalable to different digital media. PKI and the smart card system can still be used for the next revolutionary media when it hits the market, similar to when DVDs first came out.

Cons

- Smart Cards – PP-DVDs cannot be implemented until the majority of people have smart cards or the PP-DVDs come with smart cards. Smart cards are fairly inexpensive and are still coming down in price.
- Key management - Due to the use of PKI, key creation for each PP-DVD is an issue. Each PP-DVD would have to have its own set of keys. Also, a management system to reissue lost or broken smart cards or to reissue PP-DVD keys would be needed.
- PP-DVD Player – Extra hardware needed for the player.
- Standards would need to be implemented for the process if PP-DVD is to be successful. With industry standards and compliance, consumers have a much easier time transitioning to new technologies.
- The process for getting the private keys on the smart card is another management issue and will not be discussed in detail. Several options include:
  1) Smart card containing the private key comes with the PP-DVD.
  2) A one-time password, found in the PP-DVD package, which allows you to logon to a Web Authority to download your Private keys onto your own personal smart card.
  3) At time of purchase, the retailer installs keys on your smart card with your permission.
- Without further legislation protecting the consumer, solutions 2 and 3 could allow the retailer to keep a detailed list of purchases you bought, creating issues of invasion of privacy. The privacy issues dealing with smart cards are general problems that need to be dealt with outside of this paper. Privacy is one of the concerns I have with the use of smart cards,

but if proper legislation were passed, privacy concerns could be reduced or eliminated.

Nonetheless, this PKI Smart Card solution solves the three major problems of protecting the copyright owner, the consumer, and preventing piracy. By using a PKI Smart Card solution, a PP-DVD can be created and only an authorized consumer can unlock the PP-DVD. The copyright owner's rights are preserved, because only the user with proper credentials can view the contents.

Also, the consumer, with proper software, would now be able to make backup copies of his PP-DVD and encrypt the copy with the original PP-DVD keys. At no time are the copyright owner's rights violated. This encryption process will cost a little extra money to implement, but will prevent the loss of millions of dollars that pirates are currently stealing.

CONCLUSION

Legally, I can make a backup copy of my CD library as long as the data is not encrypted. With the solution I propose, it would be possible to change the DMCA such that the rights of consumers would also be protected with encrypted works. This would allow users to back up their DVDs. Currently, it is considered illegal to decrypt any encryption that protects the copyright on a DVD.

From the beginning, we set out to look at three different angles in our investigation into the rights of owners and consumers. The "fair use" rights of the consumer do not exist when it comes to DVD copying at this time. The DMCA did such a good job of protecting the copyright owners that it failed in protecting the rights of the consumer. There needs to be a change in the current system and a solution to allow for all owner and user rights both to be respected.

The DMCA, by making it illegal to produce software to decrypt the encryption system on DVDs, helps to keep the honest man honest, but it still does not prevent the true pirates from stealing. To prevent piracy, a solution similar to the one introduced in this paper would have to be implemented. PKI and Smart Cards are showing themselves to be very good way to exchange secure information across different boundaries.

Although this PKI Smart Card PP-DVD solution can't be implemented immediately because of the present limitations as discussed, it's likely that this technology will be the wave of the future. The sooner we embrace it, the easier the transition will be for everyone. With proper planning, the DVD player industry and the movie industry could work together to set standards and implement the technologies into their players and media. With proper standards and compliance with these standards, I believe consumers would enjoy the use of these technologies, as long as their rights of privacy are legally protected.

The copyright owner's rights are protected by the law and upheld in the courts. This should continue. Copyright owners should profit from their works. Also, any future copyright laws and solutions dealing with the protection of the owner's rights should not infringe on the "fair use" rights of consumers, yet should prevent piracy. There is a balance for both the copyright owner and consumer, and the Smart Card PKI Protected DVD solution will meet this equilibrium.

REFERENCES

17 US Code. Sec. 2001. Copyright Law of the United States of America. http://www.copyright.gov/title17/circ92.pdf (21 June 2002).

321 Studios vs. MGM; TriStar; Columbia; Sony; Time Warner; Disney; Universal City Studios; The Saul Zaentz Co.; and PIXAR. 23 April 2002. http://www.321studios.com/complaint.pdf (21 June 2002).

Block, Debbie Galante. "The Latch-Key Generation: Piracy Protection and DVD." September 2000. http://www.emedialive.com/EM2000/block9.html (26 June 2002).

Digital Millennium Copyright Act of 1998. H. R. 2281. 27 Jan. 1998. http://frwebgate.access.gpo.gov/cgi-bin/getdoc.cgi?dbname=105_cong_bills&docid=f:h2281enr.txt.pdf (21 June 2002).

Filzen, Keith. "The State of Digital Copyrighting." 17 February 2001. http://rr.sans.org/legal/copyrighting.php?sansrr=55752fd23c58b3f61e8d20250d77e5e8 (21 June 2002).

Hardie, Darlene Hill. "PKI: What is this thing, really?" 21 May 2001. http://rr.sans.org/encryption/PKI2.php?sansrr=7def10cc2a845db7198b2d6bb31c07d6 (25 June 2002).

King, Brad. "Tuning Up Digital Copyright Law." 16 May 2000. http://www.wired.com/news/business/0,1367,36323-2,00.html (21 June 2002).

Lucas, George. *Star Wars: Phantom Menace.* Lucas Arts Ltd. Nov. 2001. DVD

McCullagh, Declan. "Digital Copyright Law on Trial." 18 Jan. 2000. http://www.wired.com/news/politics/0,1283,33716,00.html (21 June 2002).

NDS Technologies. "A Proposal for IFE-DVD Players." 16 Sept. 1998. http://www.waea.org/tech/working_groups/dvd/1998/DVD9811B_NDS_SEC_Prop.pdf (25 June 2002).

Universal City Studios vs. Shawn C. Reimerdes. 00 Civ. 0277 (LAK). 2 Feb. 2002. http://www.dvd-copy.com/legal/universal_vs_Reimerdes-Memorandum_Opinion-020200.html (21 June 2002).

WIPO Copyright Treaty of 1996. 20 Dec. 1996. http://www.wipo.int/clea/docs/en/wo/wo033en.htm (21 June 2002).