WISE
Washington Internships for Students of Engineering

The Digital Millennium Copyright Act
Observations and Critical Questions

Max Vilimpoc
2002 WISE Intern

Prepared For the

Washington Internship for Students of Engineering
The Institute of Electrical and Electronics Engineers, Inc.

August 2002

TABLE OF CONTENTS

Introduction

The protection of intellectual property is a fundamental asset to the development of mankind. The right of authors and inventors to work freely with the potential to earn a solid living has fueled the fire of innovation from the earliest of civilization. Towards the development of our own nation, Congress was granted the authority to guarantee inventors exclusive rights to the fruits of their labor for limited spans of time.

Modern intellectual property laws inherit both a legacy of strength and support as well as a history of loose interpretation from their original ratification within the United States Constitution. Many years of legal precedent have refined the boundaries, while the never-ending march of technology has created new opportunities for clarification and confusion.

Over the course of two centuries, increasing liberalization in trade and refinement of global policies governing copyright, patent, and other forms of intellectual property have created compelling reasons for United States Government to amend copyright law. As disconnects between global and local norms for copyright and intellectual property protection grew, the United Nations officially sanctioned the creation of an organization to deal specifically with such issues.

Formally established in Geneva in 1974, the World Intellectual Property Organization works as an independent unit within the UN to harmonize the intellectual property laws and to recognize and enforce regulations evenly across 179 member countries. In 1996, the WIPO entered into agreement with the World Trade Organization (WTO), recognizing each agency’s shared interests. As a significant component of the modern global trade system, both the WTO and WIPO seek to protect intellectual property and specifically its value to industrialized nations.

In 1998, the 105th Congress passed Public Law 105-304, an amendment to Title 17, U.S.C. copyright law known as the Digital Millennium Copyright Act (DMCA). Specifically, the purpose of the DMCA was to implement the requirements of the World Intellectual Property Organization’s (WIPO) World Copyright Treaty. Failure to amend copyright law would limit the United States’ ability to participate in the World Trade Organization.

Proponents of the bill argue that it provides the right balance of legislation necessary to protect intellectual property in the new digital age. Opponents argue that the DMCA extends too much power to the copyright holders, especially regarding the digital rights of users. In light of these conflicting views, this paper will attempt to quantify the issues involved, the stakeholders, and the potential solutions available.

Overview of Copyright Law

> *"The Congress shall have Power . . . To promote the Progress of Science and useful Arts, by securing for limited Times to Authors and Inventors the exclusive Right to their respective Writings and Discoveries . . ."*
>
> U.S. Constitution Article I, Section 8, Clause 8

From our inception as a nation, the power of copyright has been codified as an essential doctrine. At its root, copyright law stems from the same mandate placed on Congress to protect intellectual works such as patents and trademarks.

In 1790, Congress passed the Copyright Act, which established an office of Copyright for the fledgling United States and officially ushered in legislative protection for American authors and inventors. Originally, American copyright law followed from the British Statute of Anne, which defined the term of copyright for authors in England. Under the Statute, authors were granted 14 years of exclusive rights to their work, after which they could renew for another 14. At the end of at most 28 years, the author's rights would be exhausted and the work would then enter the public domain.

Over the course of two centuries, successive refinement to copyright law attempted to balance the public and private interest with respect to creative freedom, fair use, profit, and monopoly. Countries independently determined their level of intellectual property protection, leading to natural disconnects and overlaps between them. Members of the global community did not necessarily respect legislative reciprocity regarding intangible intellectual property or, in some instances, even the physical products created directly from such property.

Proof of this arrived in the latter half of the 19th century as a flood of "cheap books" hit the market in America. Small American publishers abused the fact that books written by foreign writers were granted no protection under U.S. copyright law. Without fear of prosecution, the publishers could produce royalty-free prints which could then be sold at below the established market value. This practice upset the incumbent publishing houses' practice of adhering to "gentlemanly" price-fixing across international markets. (Though one could argue that the promotion of reading isn't necessarily an economic negative, either.)

As a result of these infringing acts, the international community pushed for the ratification of the Berne Convention for Protection of Literary and Artistic Works. For the first time, copyright enjoyed mutual protection among the Berne signatories, which at the time included only Belgium, France, Germany, Italy, Spain, Switzerland, Tunisia, and the United Kingdom. While it would take roughly 100 years before the United States joined the Berne signatories, within the United States several major revisions to copyright law occurred in 1831, 1909, and 1976.

Struggling to ensure that domestic artists and inventors were rewarded for their work, meetings were convened to harmonize and to synchronize national law with an international norm. Under the auspices of the United Nations' World Intellectual Property Organization, negotiations were set in motion to define international standards for the protection of copyright and other forms of intellectual property. These negotiations culminated in the ratification on December 20, 1996 of the WIPO Copyright Treaty and the WIPO Performances and Phonograms Treaty.

Overview of the WIPO Treaties

Adopted as official proposals on December 20, 1996, the WIPO Copyright and the WIPO Performances and Phonograms Treaties ("the WIPO Treaties") seek to harmonize the legislative enforcement of copyright among all of the members of the United Nations and members of the World Trade Organization. In theory, creating multilateral recognition for copyrights should create a more uniformly regulated and more competitive marketplace.

Additionally, the WIPO Treaties sought to modernize copyright law for the digital age. Creations specifically covered as literary and protected works by the treaties include Computer Programs (Article 4, WCT) and Databases (Article 5, WCT). Article 11 and 12 of the WIPO Copyright Treaty requested that member states implement legislation to effectively deal with the circumvention of technological access-control mechanisms and of rights' management systems. However, the Articles did not offer specific recommendations, leaving all authority in the decision to each member state.

Article 21 and Article 29 of the respective treaties identically specify that each treaty will enter into force three months after 30 nations ratify each. On March 6, 2002, the WIPO Copyright Treaty entered into force, followed on May 20, 2002 by the WIPO Performances and Phonograms Treaty. However, before each treaty became enforceable, member nations have the opportunity to review national laws, making amendments necessary to bring them into compliance.

Overview of the Digital Millennium Copyright Act

Passed in 1998 by the 105th Congress, the Digital Millennium Copyright Act (DMCA) aligned American copyright code with the requirements of the World Intellectual Property Organization. Specifically, the DMCA was designed to implement sections of the WIPO Copyright Treaty and the WIPO Performances and Phonograms Treaty.

Organizationally, the DMCA is split into several Titles:

Title I: WIPO Copyright and Performances and Phonograms Treaties Implementation Act of 1998
Title II: Online Copyright Infringement Liability Limitation Act
Title III: Computer Maintenance Competition Assurance Act
Title IV: Six Miscellaneous Provisions
Title V: Vessel Hull Protection Act

Of these five titles, this paper will focus heavily on those provisions created in Titles I and II.

Title I

The purpose of Title I was two-fold. First, the Title served as the legislative implementation of the two WIPO treaties regarding the protection of intellectual property of all member signatories. By passing Title I, Congress amended the text of Title 17, U.S.C., bringing U.S. copyright code into compliance with WIPO language.

Secondly, Title I implemented specific portions of the WIPO treaties regarding the technological protection of intellectual property. Specifically, Article 11 of the World Copyright Treaty (WCT) and Article 18 of the World Performances and Phonograms Treaty (WPPT) were implemented by Title I of the DMCA, which appended Sections 1201 to 1205 to the existing copyright code.

> Contracting Parties shall provide adequate legal protection and effective legal remedies against the circumvention of effective technological measures that are used by authors in connection with the exercise of their rights under this Treaty or the Berne Convention and that restrict acts, in respect of their works, which are not authorized by the authors concerned or permitted by law.
>
> WIPO WCT, Article 11. Obligations Concerning Technological Measures

> Contracting Parties shall provide adequate legal protection and effective legal remedies against the circumvention of effective technological measures that are used by performers or producers of phonograms in connection with the exercise of their rights under this Treaty and that restrict acts, in respect of their performances or phonograms, which are not authorized by the performers or the producers of phonograms concerned or permitted by law.
>
> WIPO WPPT, Article 18. Obligations Concerning Technological Measures

At the time of ratification, it was felt that the prohibition against the circumvention of technological access-control devices would enable copyright holders a means of safely marketing their properties in digital form. Removing the fear that they would be unable to seek redress for losses incurred due to digital piracy, it was believed that copyright holders would actively pursue a new global market, securely available over the Internet.

Section 1201 renders illegal the manufacture of any device capable of circumventing a technological access-control mechanism. As stated in the language of the law, the utilization of such a device is neutral to the intent of the user. Regardless of whether such a device is used to circumvent protection measures for the exercise of fair use rights, or to illegally infringe on the copyright holder's rights, the law remains neutral. At its root, the act of circumvention is sufficient to indict an individual on both civil and criminal levels.

Several exemptions are defined in §1201 that allow –

- *Nonprofit Libraries, Archives, and Educational Institutions* to circumvent access control mechanisms on commercially available materials in order to make a determination as to whether those materials should be purchased.

- *Law Enforcement* blanket exemption from liability under §1201 pursuant to authorized investigative purposes.
- *Reverse Engineering* of software technologies to allow for interoperability between separate programs.
- *Encryption Research* with the permission of the encryption authors to do so
- *Protection of Minors* in the case that certain access control measures must be circumvented to protect the minors
- *Protection of Personal Privacy*
  In the case that a technology may be gathering personally identifiable information without the consent of a user, the user has the right to circumvent security measures in order to disable the gathering mechanism.
- *Security Testing* with the permission of the encryption authors to do so

Although the exemptions were designed to allow a certain amount of circumvention and to prevent the stifling of innovation and the chilling of free speech, a number of legal cases have emerged demonstrating exactly those effects. Also of note are the extremely narrow applications for which each of the exemptions may be applied. The details of these exemptions are currently beyond the scope of this paper.

Title I also defined Section 1202 of copyright law, which created a legal space for the creation and enforcement of Digital Rights Management (DRM) information in both hardware and software. Any attempt at altering or removing the rights management information once the copyright holder determines it is considered a violation of law.

Section 1203 and 1204 define the civil and criminal penalties for the circumvention of copy control and Digital Rights Management systems.

In the following section, cases utilizing the provisions of Section 1201 and 1202 will be documented. Additionally, the merit of each case and the availability of options will be examined.

Catalog of Title I - Circumvention Cases

Motion Picture Association of America v. 2600 Magazine

In December 1999, at the request of eight major motion picture studios, the Motion Picture Association of America (MPAA) filed suit against a number of individuals, including Eric Corley, the publisher of 2600 Magazine. Despite its many years of freely publishing highly technical materials for interested electronics enthusiasts, never before had the magazine faced an injunction on its right to disseminate information.

Stemming from the fact that 2600 Magazine published an article and linked to websites describing a computer program known as DeCSS, the MPAA sought a preliminary injunction enjoining the publication of any further information. DeCSS represented the culmination of an international reverse engineering effort against the Content Scrambling System (CSS) encryption algorithm used to protect Digital Versatile Discs (DVD)s.

Developed by the Technical Protection Working Group (TPWG) of the MPAA, the Content Scrambling System is an unpublished, encryption-based access control mechanism designed to prevent the playback of DVDs on unlicensed players. Using a combination of secret encryption keys stored in both the DVD player and the DVD media, the CSS places several technological restraints on the manner in which a DVD may be played back.

A primary example of this playback control is the concept of Region Coding. According to the MPAA, the world is fractured into six distinct markets:

Region 1 - United States, U.S. Territories, and Canada
Region 2 - Europe, Japan, the Middle East, Egypt, South Africa, Greenland
Region 3 - Taiwan, Korea, the Philippines, Indonesia, Hong Kong
Region 4 - Mexico, Central and South America, Oceania, Caribbean
Region 5 - Russia, Eastern Europe, India, Africa, North Korea, Mongolia
Region 6 - China

Players licensed to operate in one region are designed not to play DVDs from other regions. The original intent of this design was to control the distribution of movies between markets across the world. For instance, a movie might be released in America to the theaters, and then released to DVD even before reaching the theaters in a foreign region. Rather than allow movie aficionados in foreign countries the opportunity to purchase the DVD directly from America for playback in their own homes, the MPAA implemented the region coding system explicitly to make such an option impossible. Region coding was also designed with a mind to prevent the widespread piracy of DVDs in countries with historically poor intellectual property protections. It was believed that by removing the ability for DVDs to be played outside of their original region, the market, and therefore the incentive for piracy would be eliminated.

Another example of the access-control mechanism at work are the control codes are used to prevent a user from skipping the standard FBI anti-piracy warning on all DVDs. However, those same control codes may make it impossible for a user to skip past movie previews or advertisements on a legally purchased DVD. Here, the consumer begins to question who actually has control over the DVD. If technologies are being applied to a DVD that limit the consumer's ability to choose what portion of the movie they wish to watch, and if those technologies are being applied such that even non-essential notices are being flagged (e.g. advertisements), then in some sense the user should have a right to reassert their right to modify, alter, and otherwise do what they want with what they own.

The claim brought forth by the MPAA was that DeCSS would be used to assist in the large-scale piracy of DVDs across the world market. However, from a technical perspective, this is an improper perspective on the actual function of the DeCSS program. Factually, the DeCSS program breaks the encryption on DVDs such that the raw movie data can be passed along to a program capable of playing it back. Functionally, this is no different than the procedure performed by a common, off the shelf DVD player as it is playing a movie.

Similarly, any standard DVD player is incapable of duplicating DVDs. Likewise, DeCSS does not in any way facilitate or simplify the disc to disc copying of DVDs. DeCSS is not a machine that takes one DVD and copies it onto another. DeCSS does not even help make the physical copying process easier. Since DeCSS does not assist in the actual, physical copying of DVDs, a question arises as to how exactly such a software program increases the level of piracy in the world market.

Instead, the focus of contention in this case is the act of reverse engineering protective encryption. The stated goal of DeCSS's creators was to develop a means by which users of the Linux operating system could play back legally purchased DVDs. Its sole purpose was to give legitimate owners of DVD media the right to view their media where they chose. However, the act of creating a piece of software capable of circumventing an access-control mechanism violated Title I of the newly instated DMCA. Thus, regardless of the intention of the user to watch a legally purchased DVD on his or her own computer, possession of the software and any of the knowledge gained in its creation was rendered illegal.

The only difference is in the fact that a player created through reverse engineering is not subject to the licensing fees of the DVD-Copy Control Authority (DVD-CCA). Prior to the release of DeCSS, there were no unlicensed DVD players on the market, meaning that each and every manufacturer of both hardware and software DVD players paid fees to the DVD-CCA for the right to legally play DVDs (since it is necessary to decrypt the video data before it can be displayed on a television or computer monitor). Essentially, the license grants a manufacturer the right to circumvent the encryption-based access-control mechanism placed on DVDs.

Herein lies another problem that has not yet been corrected by market forces. Following the release of the DVD format to the market in March 1997, the only licensed software DVD players were available solely for the Windows and Macintosh operating systems. To date, no officially licensed software or hardware DVD player has been released for the Linux operating system. Although the market of Linux users may be small, the prejudicial treatment against them by the DVD-CCA could be construed as a violation of anti-trust regulations. With regard to competitiveness, *the flexibility of a market is undermined where a single licensor exists and where only predetermined technologies are given the opportunity to succeed.*

As a technology, DeCSS was the brainchild of a group of European reverse engineers working on what was known as the Linux Video (LiVid) project. By creating an unlicensed piece of software capable of circumventing the encryption on DVDs, the DeCSS program was opening up the Linux user market for Hollywood to sell products into.

One might question the motivation of the MPAA, and whether their actions make economic sense. Does it make sense for a weak encryption and content protection system to be protected by government legislation against traditionally legal reverse engineering? Or, does this protection disrupt the natural cycle of innovation in which the weaknesses of any given design are initially exploited but ultimately cauterized in subsequent revisions?

It must be noted that 2600 Magazine was not the creator of the DeCSS program. Instead, the magazine simply provided information about the software's existence, as many other news outlets would do in the weeks following its release. An injunction against 2600 Magazine's ability to provide information to its readership seemed to be in violation of its First Amendment protection as an agency of the press.

From the perspective of actors and directors, does it make sense to trust incredibly valuable media and intellectual property to diminutively weak forms of technological protection and excessively strong forms of legislative protection? Does it also make sense to attempt to segregate and treat a vast global marketplace as a segmented, limited market, in which certain countries receive goods before others? Does it not make more sense instead to seek the largest viewership possible, across continents, languages, operating systems, or any other difference? Ultimately, the goal of the DVD industry should be simply to sell an unrestricted product at reasonable prices to the most people as possible, rather than attempting to secure a fine-grained market monopoly and control over what devices people use to view their content.

The question that must be posed is: Is this economically sensible?

The time has come for a more sensible business model to emerge. The scenario of widespread piracy accompanied by lost profits and lost movie revenues has already emerged regardless of whichever ineffective technological barricades are erected. While the increasing deployment of the Internet to numerous foreign countries is itself a neutral activity, the rapid proliferation of movies to foreign countries has resulted in speculatively large losses to domestic movie studio profits.

It doesn't have to be this way. Movie studios, in the course of production and post-production of their summer blockbusters, or indeed any of their movies, could simultaneously subtitle and/or redub their titles for foreign markets. Rather than *delaying* the release of a single movie in multiple marketplaces, the movie industry could instead release a feature film *simultaneously* to the global marketplace. Arguably, this model would not make sense across the entire gamut of movies produced in the United States, as movies do not always recoup their initial costs. However, this process of *globalizing* movies could simply be applied to those movies which bear the most semblance to blockbuster potential.

Let us examine the historical state of the global media marketplace.

Initially, a movie was released exclusively to the American theater system. The movie would stay within the confines of the domestic market for potentially several months while being prepared for a foreign release. In the interim, videocassettes would be assembled and readied for release to the American market, sometimes even before the foreign release.

At the time, the function-neutral factors that enable the rapid dissemination of copyrighted video were not yet in place. Camcorders and other portable video recording mechanisms were too bulky to conceal in movie theaters. At dialup connection rates, the Internet was not a feasible transport method for the massive amounts of data required by movies. Additionally, no algorithms capable of compressing video data down to manageable sizes had yet been invented.

Let us examine the current state of the global media marketplace.

Again, the movie is first released into the American theater system. After a number of weeks headlining at the box office, a translated movie version may be released to foreign markets. In the meantime, DVDs are packaged and produced, with extra features and additional bonus materials collated into the final product.

Several factors are now in places that dramatically alter the business and technical landscape. Camcorders and other portable video recorders have seen immense innovation both in terms of video resolution and physical size reduction. An order of magnitude increase in the speeds at which home users are capable of accessing the Internet has made rich content available to a larger population than ever before. Additionally, vast improvements in compression algorithms allow more video to be stored in less space than ever before.

It should be kept firmly in mind that none of the advanced technologies above are necessarily charged with a moral responsibility to prevent the piracy of copyrighted materials. Their very existence does not justify the call for mandates on technology that may ultimately restrict their substantial non-infringing purposes. Many of the advancements in camcorder technology, computer processors, video compression, and broadband, have been achieved and pursued at the behest of a user base wanting to do more with the myriad of media they have already freely purchased and produced.

The argument here is an appeal to consumer choice. People around the globe want American media, but the major media conglomerates refuse to extensively and efficiently globalize their operations. By offering choice to the consumer of a foreign country, indeed, by offering a foreign national the option of watching the first release of a new movie on the same day as any American citizen, for a comparable price, can any economist doubt that a foreigner would be willing to pay a fair market price?

Therefore, the advancement of technology has rendered both the business model and the traditional movie release schedule obsolete. In the present day, within a matter of hours after its release, a bootlegged copy of the movie may be made available on the Internet for consumption. Within a matter of days, a subtitled version of the movie may already be available in a number of international markets. The question, then, that the global consumer should ask themselves is: if the pirates are able to rapidly reformat and repackage a piece of media with the assistance of powerful digital video tools, high speed communications, and large amounts of enthusiasm – *at zero cost* – what is keeping the copyright holders from following suit?

At its crux, the studios should realize that broadband Internet access is not damaging their marketplace. Instead of treating high-speed customers as a liability, the major motion picture studios should treat broadband Internet access as an asset, with each new broadband user a potential media consumer.

In this modern era of immense connectivity, it is not the technology that should be faulted, but the mechanisms of the market for failing to keep up.

United States v. Sklyarov

On July 16th, 2001, after delivering a presentation on his successful efforts to reverse-engineer the weak encryption used to protect Adobe eBooks, Russian math and cryptography student Dmitry Sklyarov was arrested as he was leaving the DefCon computer security conference in Las Vegas. Sklyarov had come to the United States to present his findings to a conference of computer security professionals, whose interests could be considered both academic and practicable in nature. In a series of twenty-slides, Sklyarov documented the weak security measures that he had discovered being utilized in several supposedly secure eBook file formats.

In some cases, Sklyarov discovered that the protection offered by commercial eBook security products amounted to little more than gradeschool-style encipherment. Yet, these security packages were being sold as reliable electronic theft deterrence measures to eBook publishers for several thousand dollars apiece. As part of his employment at ElcomSoft Co. Ltd., Sklyarov worked on a product known as the Advanced eBook Processor, which could be used to remove the usage restrictions on Adobe eBooks.

As part of their specification, eBooks can have various usage restrictions embedded, which can prevent users from utilizing them in various ways. The amount of text that can be copied from a page, the number of pages that can be printed, the number of copies that can be made, the number of hours a document may be read, and other aspects can be specified during the creation of an eBook. Proponents of fair use rights argue that these access-control restrictions impinge on the rights of owners to utilize eBooks in a manner consistent with traditional paper books. On the other hand, eBook vendors argue that the consumer is allowed finer control over how they wish to utilize their eBooks, in addition to allowing vendors to offer multiple versions of the same product at different price levels depending on which restrictions are enabled or disabled.

There are several points of contention at large in the case against Sklyarov. First, if a researcher conducts all of their research in a sovereign nation that is not subject to the terms of the United States' copyright law, should that person be held liable upon entry into U.S. jurisdiction? Second, what effect will there be on innovation if reverse-engineering and cryptographic research are subject to criminal prosecution under Title I of the DMCA? Third, how will profits be affected by the discovery of weak encryption systems? Should weak encryption be protected, or should publishers consider litigation against providers of weak encryption systems for potentially lost sales due to piracy?

While Russia is subject to the terms of the Berne Convention[1] on international copyright law[2], unclear is the extent to which *access-control* mechanisms are governed by such law. Indeed, the research that Sklyarov was performing did not constitute a violation of Russian copyright law. As a matter of fact, Article 25 of the Russian *Law on Copyright and Neighboring Rights* explicitly grants programmers the right to reverse engineer software for which they have had no previous exposure to source code in order to improve interoperability with products of their own design.

2. Any person lawfully in possession of a copy of a computer program may, without permission from the author or any other owner of exclusive rights, and without paying any additional remuneration, reproduce or convert the object code making it into a source code (decompile the program) or have such acts performed by third parties, if they are essential to ensure the interactive capabilities of a computer program independently created by that person with other programs compatible with the program so decompiled, in which case the following conditions have to be fulfilled or observed:

(1) the person concerned must not previously have had access to other sources capable of providing him with the information necessary to ensure the interactive capability;
(2) the acts mentioned must only be performed in relation to the parts of the computer program the decompilation of which is essential to the achievement of the interactive capability;

Article 25, Section 2, Decompilation of Computer Programs,
Russian Law on Copyright and Neighboring Rights

However, the law does prohibit the creation of 'comparable software' from the information gathered via the reverse engineering process. In a more conventional sense, the protection of reverse engineering is similar to rules against plagiarism. On the one hand, an author, a student, or a researcher may read many items related to his or her particular interest. However, when the time comes to produce a novel, a research paper, or a new journal article, none of the individuals is allowed to create a writing that mirrors or could be mistaken for any of the items of *prior art*. Instead, the individuals are granted rights to quote and refer to previous authors and to synthesize new ideas that may have been inspired by knowledge gained.

In the case of ElcomSoft's Advanced eBook Processor (AeBP), Sklyarov was simply analyzing the eBook file format to determine weaknesses in its protection system. Prior to the passage of the DMCA, such curiosity was not subject to civil or criminal penalties. Upon discovery of the simplicity with which eBooks attempted to attain security, Sklyarov believed it was important to inform the Internet community at large. As a trained cryptographer, Sklyarov was operating in a manner consistent with his occupation. Full disclosure of potential and actual faults in cryptographic systems is a commonly accepted practice that ultimately guarantees the integrity of the strongest.

While it is true that the use of the AeBP makes it possible to convert legally purchased, copy-protected eBooks into the open and unprotected Portable Document Format (PDF), the nature of the tool itself does not inherently promote piracy or illegitimate use. In this case, the intentions of the user and of the technology are conflated. By allowing a user to move an eBook between computers, make backup copies, and print limited portions for personal, non-commercial use, the AeBP actively restores to digital texts what are considered traditional fair use rights. In the realms of literature and books, those fair use rights are generally identical to those available with physical books.

United States v. ElcomSoft Co. Ltd.

After dropping its charges against Russian programmer Dmitry Sklyarov in exchange for a plea bargain to testify against his employer, the Department of Justice shifted the weight of his case onto the Russian software firm ElcomSoft Co. Ltd. (ElcomSoft). According to the provisions of Title I of the DMCA, as codified in §1204 (a), "Any person who violates section 1201 or 1202 willfully and for purposes of commercial advantage or private financial gain" can be held liable and fined up to $500,000 with the potential for up to a 5 year prison sentence.

ElcomSoft became liable under the DMCA because they sold copies of their Advanced eBook Processor to customers in the United States through the Internet. There is some question, however, of the legality and applicability of U.S. copyright law against foreign corporations. Do the international treaties on copyright bind one country to another country's code? In addition, should the restrictive measures of the DMCA be allowed extraterritorial jurisdiction, in effect creating a blanket authority over other countries' copyright enforcement procedures? Ultimately, neither the treaty arising from the Berne Convention on Literary and Artistic Works nor the WIPO Copyright Treaty define the legal boundaries of copyright law. Therefore, in the case of ElcomSoft, the United States has the authority to pursue its lawsuit within its territorial boundaries.

Another curious issue is the selectivity with which the DMCA operates. Fuzzy, undefined legal boundaries exist as to which activities constitute fair use exceptions and which are immediately subject to criminal penalties. An unfortunate side effect of the ElcomSoft suit is a growing culture of fear that has altered the nature of security research on the Internet. Those individuals who may produce any sort of software at all that might be used in the circumvention of any access-control mechanism have become fearful of the repercussions of American law. Around the world, a number of security researchers have already repressed the release of information out of fear of liability under the DMCA.

The curiosity is this: If individuals invest their time and effort in determining the weaknesses of an access-control system, and they are capable of defeating it, they have one of two options now under the DMCA. Publishing the knowledge gained through their research and taking credit for that knowledge may subject them to civil and criminal penalties. Publishing anonymously would keep them from assuming liability. Unfortunately, this present state of affairs is incompatible with a rich view of liberty. One of the foundations of our liberty is the right to freely identify with one's own speech and ideals. When individuals are given only a few options as to their method of expressing themselves, then the ideals of freedom are being severely curtailed. If this curtailing of First Amendment guarantees begins to have noticeable effects on the quality of the public domain and public discourse, it becomes more difficult to justify the existence of laws such as the DMCA and to ignore the chilling effect on speech.

Ultimately, regardless of whether the individual opts for anonymous or identified release, the knowledge makes its way onto the Internet. Unfortunately for some, and fortunately for others, containing ideas on the Internet is exceedingly difficult. Knowledge is indifferent to the statutes that attempt its containment. At the point of its release, it does not matter whether the information was leaked for profit or for personal interest; the secret knowledge is no longer subject to the control of the researcher or its original creators.

The only difference between an anonymous and an identified release is the target of liability. Because an individual identified himself as the creator of a work that circumvented or reverse engineered an access-control mechanism, he is immediately subject to the actions of copyright law. But if that individual opted to give up the rights to identify himself with a work of reverse engineering, i.e. their moral rights as an author, he then is less likely to be subjected to liability. This is an unfortunate turn of events for those of curious constitution, because it frustrates the discovery and elimination of faults in any number of digital systems. Essentially, the DMCA's exemption for encryption research fails to protect the researcher and instead protects the incumbent encryption scheme against attack.

Imagine for a moment that as a car owner, you discover faults in the design of a braking system while performing routine maintenance on it. You want to report the problem to the proper authorities but according to the law, you were not allowed to take the tire off the car in the first place. So you could be subject to liability if you report the problem because of the implicit removal of an access-control mechanism (the tire, hypothetically). What do you do? You clandestinely establish a repair service for other owners and charge a small fee for labor. Now you are opened up to criminal liability because, while you are performing a needed service, you have willfully engaged in business that involves access-control circumvention (removing the tire).

For those individuals who make careers out of discovering the flaws in software, the DMCA spells a death knell for their research. Although §1201(g)(2) defines the 'Permissible Acts of Encryption Research', the provision of §1201(g)(2)(C) states:

"the person made a good faith effort to obtain authorization before the circumvention."

Effectively, this clause nullifies the usefulness of the entirety of §1201(g), by virtue of the fact that the encryption researchers must now obtain permission in writing prior to their investigation. From a legal standpoint, if a researcher is unable to clearly enumerate exactly the sort of flaw being researched, they may find themselves in violation of the DMCA. As well, it is paradoxical for a researcher to know the flaw being sought before permission to circumvent is requested.

A basic assessment of the case against ElcomSoft reveals its focus on the dual use nature of technology. What ElcomSoft was selling was in some ways similar to a set of workshop tools. The tools constitute no moral authority or will in and of themselves. On the one hand, a socket wrench might be used by thieves to illegally disassemble a car in a chop shop. On the other hand, a mechanic might use the tools to fix an automobile. In either case, the tools should not be colored by the intent of their owners.

A better example might go something like this: Imagine a book that requires special glasses to read because the words are jumbled into unreadable ciphers in plain sight. At some point, a friend asks you if he can borrow the book to cite a few paragraphs from it for his research report. You decide that you can't lend him either the book or the glasses, but you want to make a copy of the paragraphs for him. Unfortunately, the photocopier will only copy the jumbled text if you try to use it. So you come up with a special lens for the photocopier that will unscramble the text of the book. You copy the page containing the text needed by your friend, and then put the special lens away. In substance, the Advanced eBook Processor operates in an identical manner to the lens. It allows the owner to make legitimate fair use of his or her property.

Another issue at stake in this application of intellectual property law versus the rights of fair use is that indeed, the DMCA circumvents a user's expectation of due process. The presumption of legality and substantial non-infringing use is itself circumvented in favor of the worst-case scenario, that a particular tool or device is used for illegal purposes, without ever consulting the context of the situation. This was not the original intent of copyright law, which was designed upon the premise of punishing for infringement after the fact, not for preemptive restraint.

What we know from history is that precedent is not in favor of outlawing devices that *may* have the potential for illegal use. Were this the case for countless scores of other inventions such as: guns, knives, rope, pickaxes, cars, and the like, much of our modern society would be deemed too dangerous for public consumption. Why then are tools for access-control circumvention deemed so threatening?

Secure Digital Music Initiative v. Felten

On September 6, 2000, the Secure Digital Music Initiative (SDMI) kicked off its "Hack SDMI" challenge, an open invitation to security researchers to determine whether flaws were present in four endorsed digital watermarking technologies[3]. Watermarking technologies have been proposed as a method by which Digital Rights Management instructions can be coded into secured audio files. Theoretically, the removal of watermarks from digital media should be difficult, such that the quality of the media degrades significantly if removal is attempted. As a reward for the efforts of participants, the SDMI offered a prize of $10,000 for successful and reproducible attacks. For those participants seeking remuneration for their efforts, the SDMI required that all intellectual property rights for knowledge gained during the research process be assigned to the SDMI in the event of a successful attack.

However, for those participants not seeking monetary compensation for their efforts, the requirement to transfer intellectual property to the SDMI would not be in force. Instead, a purely voluntary disclosure of research knowledge was requested via the Click-Through Agreement[4] on SDMI's challenge website: "You may, of course, elect not to receive compensation, in which event you will not be required to sign a separate document or assign any of your intellectual property rights, although you are still encouraged to submit details of your attack."

As an exercise in computer science and applied research, Professor Edward Felten of Princeton University, along with colleagues from Rice University, decided to *accept* the challenge to crack the SDMI watermarking technologies and to *decline* monetary compensation. Thus, Felten felt no obligation to withhold his research once it was complete because it was clearly stated in the terms of the Click-Through Agreement for the SDMI Public Challenge that he did not have such responsibilities.

What Felten encountered instead was a legal firestorm over his proposed presentation titled "Reading Between the Lines: Lessons from the SDMI Challenge,"[5] which he was slated to present at the 4th International Information Hiding Workshop Conference[6] in April 2001. By detailing the processes employed by watermarking technology to secure digital music files, and not remaining silent about his research, Felten found himself under threat of legal action[7] based on his circumvention of an access-control mechanism. Utilizing the DMCA §1201(a) provisions, the SDMI sent a letter on April 9, 2001, warning of legal consequences should Felten publicly release his findings.

Under pressure from the recording industry-backed SDMI, Felten decided to limit his potential liability and to prevent exposing colleagues, university backers, and the conference organizers to legal threat. On April 26, 2001, Professor Felten read a prepared statement[8] explaining his group's decision to forego presenting their academic research until the legal issues had been settled. On June 6, 2001, the Electronic Frontier Foundation, in concert with Professor Felten, filed suit against the Recording Industry Association of America (RIAA), the Secure Digital Music Initiative (SDMI), Verance Inc., and the Department of Justice, seeking a Declaratory Judgment on the legality of presenting scientific findings regarding the successful defeat of digital watermarking technology in the context of a security conference.

By the date of the lawsuit filing, Felten's paper had been accepted for presentation at the USENIX Conference, an annual conference related to many diverse computer-oriented disciplines. In order to be selected, Felten's paper was subjected to the standard peer review process to ensure that it had merit as technical and scientific research. By requesting a Declaratory Judgment, Felten, with the backing of all but one of the original researchers and the support of the USENIX Association, sought legal protection of his First Amendment right to present his paper at the USENIX Conference.

On July 12, 2001, the RIAA filed a motion to dismiss the case, arguing that they had never threatened a lawsuit against Professor Felten. In the meantime, the EFF was busy gathering declarations from a number of noted computer scientists regarding the chilling effect on speech that was being felt worldwide. On August 15, 2001, without a judgment in the case, Felten faced potential arrest by presenting his research to a crowded auditorium of security researchers. The threat seemed very real, as exactly one month before, Dmitry Sklyarov had been arrested for breaking Adobe's eBook scheme. In late September, with the proverbial chicken let out of its coop, the Department of Justice filed a motion to dismiss EFF's case, stating their belief that the case lacked merit.

A serious consequence of the U.S. v. ElcomSoft and SDMI v. Felten cases has been the withdrawal of scientific research from the global community. Because of the sensitive nature of their research, a number of researchers worldwide have withdrawn their research for fear of the unlimited lifetime of liability they might face in traveling to the United States. Also, since many scientific conferences charge attendance fees to cover costs, conference organizers are subject to potentially criminal penalties under the current rules. Title 17 U.S.C. §1204(a) states that: "Any person who violates section 1201 or 1202 willfully and for purposes of commercial advantage or private financial gain" may be fined up to $500,000 and imprisoned for up to 5 years. Unfortunately, the interpretation of what constitutes commercial advantage is vague enough that it may include conference organizers who may simply be covering the costs of hosting a large forum for academic research. As a result, a number of conferences have considered moving offshore in order to extract themselves from liability and scrutiny under the DMCA.

Ultimately, the security community is worse off when free and open discussions involving sensitive topics are potentially rendered illegal.

Norway Economic Crime Unit v. Johansen

Parallel to actions in the United States in the MPAA v. 2600 Magazine case, allegations of criminal conduct were brought against Jon Johansen and his father Per Johansen in Norway by the Norwegian Motion Picture Association (MAP) and the U.S.-based DVD-Copy Control Association (DVD-CCA)[9]. Due to the fact that Jon Johansen resided in Norway during the creation of the DeCSS program and due to the fact that he did not charge money for or seek financial gain from the creation of his program, he could not be charged under the same statutes that are currently being used against ElcomSoft Co. Ltd..

The case is founded upon the Section 54 provisions of Norwegian Copyright Code, which outlaw the "sale of or possession for purposes of gain, of any means the sole purpose of which is to facilitate the unlawful removal or circumvention of technical devices for the protection of a computer program". Another provision within the same section states, "Any person who willfully or negligently is an accessory to any infringement specified in the first paragraph shall be liable to the same penalty."

Also, the case is founded upon Section 145(2) of Norwegian Criminal Code, which prohibits a person from accessing data for which they have no permission. Initially, the law was designed to allow enforcement against unauthorized intrusion into computer systems by third parties. Ostensibly, the argument is that circumvention of the encryption protecting DVD movie data constitutes a violation of the law.

For the purposes of this case, neither statute seems to be specific enough to justify criminal charges against either Jon Johansen or his father. Since neither of them profited from distribution of the DeCSS program, the enforceability of Section 54 provisions is questionable. Secondly, because Section 145 is vaguely defined (or vaguely defines rights of ownership) it is unclear whether the penalties apply to the *owner* of a DVD. Interpreted from another perspective, applying Section 145 against a DVD owner is substantively similar to prosecuting an individual for breaking into his or her own home.

At a more fundamental level, the case raises more important questions of ownership and the reasonable expectations of property holders. Primarily, the question of who owns the content *on* the DVD is at the center of the argument. There are two positions currently being fought over by opposite camps. First, there is the view that there is a separation between ownership of the content on the DVD and ownership of the physical DVD. Proponents of this view believe that by purchasing a DVD, a person is assigned the rights to play it back only on an officially licensed device and in a manner mandated by the content creator. In this view, the person owns the physical storage medium, but not its contents. In essence, a person has only the license to view the contents. Second, there is the view that there is no separation between the physical and intellectual components of the DVD. Proponents of this belief argue that when a person purchases a DVD, their fair use rights allow them ownership and substantial non-infringing uses over both the medium and its contents.

One final question: What is the difference between taking a physical pen and drawing on the surface of the DVD, and taking a segment of video off of the DVD and drawing on it with a virtual paintbrush?

Title II: Notice and Takedown

Title II of the DMCA, the "Online Copyright Infringement Liability Limitation Act", provides a means by which Internet Service Providers (ISPs) may indemnify themselves against penalties arising from copyright infringement occurring on their network. Commonly referred to as "notice and takedown", the procedure defining the necessary legal actions of the plaintiff and defendant has encountered challenges on Constitutional grounds.

Under the provisions of Title II, the liability of Internet service providers (ISPs) against infringement of copyrighted traffic is limited, given that certain conditions have been met. Meeting these conditions enables the creation of a so-called 'safe harbor' in which an ISP is indemnified both from the claims of the copyright holder and from the claims of the alleged infringer.

One issue of primary importance that has arisen from the implementation of Title II has been the improper application and potential abuse of the "Notice and Takedown" procedure. While the constitutionality of the procedure has not yet been called in for judicial review, a chilling effect on free speech has been felt on a widespread basis by a number of Internet users.

The mechanism by which Title II operates is this: If a copyright holder detects a potential infringement in content found on the Internet, the holder has the right to seek damages from the alleged infringer. In order to eliminate liability for storing potentially infringing content on their computer servers, the service provider is notified and given a fixed number of days to remove the itemized content or be subject to the same liability as the infringer. Regardless of whether the content is or is not infringing, the service provider is subject to liability if it does not comply with the Notice.

Herein lies a problem with Title II. In Near v. Minnesota (1931), the Supreme Court ruled that the publication of material could not be enjoined regardless of its potential for scandal and public upset. Paper copies of newspapers bearing potentially libelous material could be distributed for general consumption without prior restraint. Only in situations of unprotected speech or speech related to national security could the application of prior restraint be made.

Title II has made possible the restraint of free speech by offering service providers a single safe option against financial loss. Rather than risk indictment on contributory infringement charges, service providers are avoiding lawsuits by immediately removing both infringing and non-infringing materials alike. However, the determination regarding whether materials removed are actually infringing may never be made. In this light, the mere threat of having to share the burden of a legal defense is sufficient to censor a legitimate means by which free speech may be made.

It may be argued that someone who is interested in placing on the Internet potentially infringing content such as criticism, parody, or other protected First Amendment expressions has many options and outlets to do so. However, with the provisions of Title II, that individual may find themselves needing to seek web-hosting services outside of the jurisdiction of the DMCA. In a manner of thinking, the value of free speech diminishes if it becomes increasingly difficult to speak under the jurisdiction of a law that does not require actual proof of infringement.

Subsequently, one of the major unintentional consequences of Title II is that it may often provide summary judgment for the plaintiff if his or her Internet Service Provider immediately removes allegedly infringing material.

Catalog of Title II - Notice and Takedown Cases

Unfortunately, because of its efficacy, Title II provisions have rarely been challenged in court. For the most part, the cases listed here are categorized as the result of Cease and Desist orders that have been issued to alleged copyright infringers and not necessarily as official court case references.

Church of Scientology v. Google, Inc.

Citing the notice and takedown provision of the DMCA, the Church of Scientology filed notice with Google, Inc. over their indexing and linking to a website known as Operation Clambake (www.xenu.net) which held highly critical views of the religion. The Church argued that the unauthorized use several pages of religious text, even in a piece of criticism that is traditionally protected by the First Amendment, violated their intellectual property rights. Therefore, as an act of infringement, both Google and the operators of xenu.net were served with the terms of Title II of the DMCA.

Google's role was as a contributor to infringement. As a search engine, they linked to and cached several of the pages cited in the Notice as infringing the Scientologist's copyright. Initially, Google's response was to remove all links to the xenu.net web page, including pages cited in the Notice, but also exceeding the original demands. By removing a link to the home page of the xenu.net website, Google effectively cut all references to a website with other potentially legitimate content.

As the story began to spread across various web news outlets, a number of websites across the Internet began linking to the xenu.net website. In addition, Google came under pressure from numerous groups to re-link the home page of xenu.net because it was not specifically listed as a potentially infringing document. Finally, after receiving pressure from free-speech advocates about the precedent of their action, Google restored the link to the xenu.net home page. However, enough alternate indexed routes had been established to the xenu.net pages that containing knowledge of the site's existence became increasingly difficult for the Church of Scientology.

Blizzard Entertainment v. bnetd Project

In 1998, responding to a need for multiplayer server software for several of Blizzard's gaming titles, the bnetd project was begun to allow players to set up servers under their own supervision. Previously, the users of games such as Starcraft, Warcraft, and other Blizzard games were only offered the choice of connecting to Blizzard's official servers hosted in the United States. For foreign citizens, the delay in transmitting gaming data made for a less enjoyable gaming experience. In addition, gamers in countries that levy tariffs on international faced the additional fees as a consequence of accessing the Internet.

The bnetd project sought to alleviate these problems by reverse engineering the protocol used to transport the realtime gameplay information between client and server. By independently creating a software package that was interoperable with existing games, the bnetd project was giving gamers more flexibility and options as to how they would be able to play their multiplayer games. Theoretically, the reverse engineering provision of the DMCA offered enough breathing room for the developers.

On the opposite side of the legal table, Blizzard Entertainment argued that the bnetd program would allow users of pirated copies to play multiplayer games without having to go through the authentication measures that Blizzard's gaming service, known as battle.net, provided. In sum, there would be no way for Blizzard to enforce its anti-piracy measures if it lost control of the authentication process.

Battle.net, the Blizzard multiplayer gaming service operates by checking to make sure that no two players are logged in using the same unique identifier. The claim against the bnetd developers is that their software represents a circumvention device against an access-control mechanism and is therefore illegal under the DMCA. However, what differentiates this example from previous examples is the fact that Blizzard attempted to silence the developers using the Notice and Takedown provision against their web service provider before seeking legal action against their reverse engineering actions.

As of the writing of this paper, the action against the bnetd developers has not resulted in the removal of their software or their website.

Conclusion and Recommendations

Tasked with the intent of updating copyright law to address the digital era, the Digital Millennium Copyright Act has seen many legal challenges to its Constitutionality. In the four years since its passage, numerous cases have been filed both in support of and in opposition to the copyright clauses created by the DMCA. Answers to questions regarding the national and international scope of copyright law, its enforceability, potential chilling effects on speech, and other unintended consequences, are being actively being sought in both the legislative and judicial chambers of government.

From the issues raised in the first section of this paper, however, it is apparent that some measure of amendment may be necessary in order to ensure that innovation, creativity, and the very ideas which copyright intends to protect are not cut short unintentionally. At present, the use of anti-circumvention legislation against researchers in the fields of computer security and encryption has resulted in a more restrictive marketplace of ideas. Even in sovereignties traditionally not subject to foreign copyright law, the effects of transnational copyright enforcement and pressure from global trade organizations are being felt among academic researchers. In the shadow of the arrest of Russian cryptographer Dmitry Sklyarov, and threats against Norwegian teen Jon Johansen, a number of international researchers have foregone the publication of research in order to keep themselves safe from potential liability.

Ultimately, the removal of freedom in academic forums leads to less innovation, and less technological development as a society. Legislators must take care that in providing for the needs of one interest, they do not unintentionally harm the strengths and the foundations of others.

There are a number of potential solutions available at present, among which two potential amendments to the copyright law may be appropriate.

While it may harm the content producing industries to remove the anti-circumvention clause from U.S. copyright law, it has been proven time and time again that Section 1201 of the DMCA has not been effective in diminishing the level of piracy available across the wide spectrum of Internet distribution methods. Instead, the sorts of precedents that have been established have been cases against individuals exercising their fair use rights, performing some sort of cryptological research, or even participating in legitimate, industry-sponsored challenges. Since the applications of Section 1201 have somewhat favored offensive rather than protective measures, the time has come for the legislature to reconsider whether or not the law is effective and appropriate.

Rather than removing the anti-circumvention language, amending it to allow for less restrictive fair uses might be an appropriate action. Allowing for activities that would not be misconstrued as infringing activities by the content industries, and especially for the protection of academic studies involving circumvention of access-control mechanisms would result in positive benefit overall for the content industries. The foundations of strong digital security systems rely on the testing and retesting of existing systems towards the formulation of their progeny.

A third solution might be the maintainance of the current status quo, which would simply give the courts time to observe and set legal precedent on new cases. Unfortunately, it is not the recommendation of this paper that this course of action be taken, for a number of reasons. First of all, the current balance of copyright is tipped steeply toward the side of copyright holders. The defensibility of fair use is not well established, especially with regards to circumvention for the *purposes of fair use*. Secondly, the balance of law is strongly tipped toward the copyright holders, who traditionally have a much larger finance base than the alleged infringers. While the intent of justice is to remain blind to the influence of each party's finances, such influence is ultimately felt throughout the judicial system.

As a matter of course, then, a legislative amendment would be favorable towards restoring the ability of researchers, consumers, scientists, students, and many other interests to make full and fair use of the copyrighted goods they purchase.

Supplementary Definitions

Fair Use

Counterbalancing the exclusive rights of authors and publishers, numerous legal battles have been fought with the intent of securing for the public certain usage rights and expectations regarding copyrighted materials. The principle of *fair use* embodies these rights and expectations, allowing the public to utilize copyrighted goods in a myriad of ways that do not ultimately infringe on the publisher's commercial interests. Fair use is not a tightly defined legislative principle; rather, its boundaries are primarily determined through the interpretation of courts.

The establishment of fair use principles by Folsom v. Marsh implicitly defined the right of users to use legally acquired, copyrighted materials in ways the publishers never intended. The question of whether or not these uses were legitimate would be left up to the court system to decide as new cases and challenges of infringement arose. Important to note is the recognition that publishers are not granted an exclusive monopoly on future ideas that might stem, in part, from current works. Without the right to innovate upon previously established creative works, countless authors, critics, and artists might have lost their creative license and instead been subject to intense pressure to conform to a strict interpretation of copyright law.

Codified as Section 107 of U.S. copyright law, the fair use doctrine is a loosely defined set of criteria used to determine whether or not the use of a literary or artistic work by someone other than the copyright holder constitutes infringement. Four factors are considered:

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

These factors form the foundation used by the courts to distinguish fair use from infringement. In some ways, the looseness of the interpretation of copyright law is similar to the intent of the Ninth Amendment: All of the rights not specifically reserved for the copyright holder are preserved for the end user.

Injunctions

As defined in the Federal Rules of Civil Procedure, Rule 65, an *injunction* is a court order requiring that a defendant perform some action in order to maintain a pre-trial status quo or to prevent a potential further injustice from occurring[10,11].

Prior Restraint

The doctrine of prior restraint is defined as the enjoining of first amendment rights before their use by an individual or group. While exceptions have been made in very specific instances, the application of prior restraint is subject to intense scrutiny due to potential conflict with first amendment liberties. The potential for abuse and the ensuing chilling effect on speech have traditionally given the legal system strong grounds for caution before any application of prior restraint.

A landmark decision against the application of prior restraint was handed down by the U.S. Supreme Court in the Near vs. Minnesota (1931) decision. As a rule, the justices decided, the restraint of speech of grounds of its *potential* to cause damage is unconstitutional. Instead, the justices argued that the potential for punishment under well designed and tested libel laws after the fact served as sufficient deterrent from abuse of the First Amendment.

Circumvention

circumvent (tr. v.) To go around, bypass[12]. In the context of this paper, circumvention refers to the bypassing of technological access-control measures often employed to protect copyrighted materials from unauthorized, but potentially fair uses.

Circumvention Devices

Devices, both hardware and software, designed to circumvent access-control mechanisms. Under the DMCA, these devices are for the most part outlawed, with a few very limited research exceptions

Bibliography

Copyright & Fair Use: Primary Source Documents, Stanford University Libraries, http://fairuse.stanford.edu/primary/

World Intellectual Property Organization
http://www.wipo.int/

About WIPO
http://www.wipo.int/about-wipo/en/

Intellectual Property Protection Treaties
http://www.wipo.int/treaties/ip/index.html

WIPO Copyright Treaty, Ratified December 20, 1996
http://www.wipo.int/clea/docs/en/wo/wo033en.htm

Press Release PR/2002/304
http://www.wipo.org/pressroom/en/releases/2002/p304.htm

Bill of Rights, U.S. Constitution, National Archives, http://www.archives.gov/exhibit_hall/charters_of_freedom/bill_of_rights/bill_of_rights.html

“Talking Smack: Copyrighting the Future”, David Nagel, Digital Media Designer Magazine, http://www.digitalmediadesigner.com/2002/06_jun/editorials/smack98.htm

Copyright 101 for the Digital Domain, Brian A. LaMacchia, http://www.farcaster.com/presentations/copyright-drei97/index.htm

Copyright Law of the United States of America, Title 17, U.S.C.
http://www.copyright.gov/title17/

Chapter 12: Copyright Protection and Management Systems, Title 17, U.S.C.
http://www.copyright.gov/title17/92chap12.html

Digital Millennium Copyright Act
Public Law 105-304 -- October 28, 1998 -- To amend title 17, United States Code, to implement the World Intellectual Property Organization Copyright Treaty and Performances and Phonograms Treaty, and for other purposes.

Copyright Timeline, Association of Research Libraries
http://www.arl.org/info/frn/copy/timeline.html

EFF "Intellectual Property: MPAA DVD Cases" Archive
http://www.eff.org/IP/DMCA/MPAA_DVD_cases/

MPAA Members' Complaint in MPAA v. Reimerdes, Corley and Kazan
http://www.eff.org/IP/DMCA/MPAA_DVD_cases/20000114_ny_mpaa_complaint.html

Testimony of Michael Einhorn in Universal City Studios Inc. v. Reimerdes, pp. 1035
http://www.eff.org/Legal/Cases/MPAA_DVD_cases/20000725_ny_trial_transcript.html

Testimony of David Touretzky in Universal City Studios Inc. v. Reimerdes, pp. 1084
http://www.eff.org/Legal/Cases/MPAA_DVD_cases/20000725_ny_trial_transcript.html

Content Scrambling System (CSS): Introduction, Gregory Kesden, Carnegie Mellon University,
http://www-2.cs.cmu.edu/~dst/DeCSS/Kesden/

DVD Regional Coding Map & Information
http://www.laserrot.com/info/lrinfo/dvdmap.html

OpenDVD.org
http://www.opendvd.org/
A Brief History of DVD
http://www.cdpage.com/DVD/dvdhistory.html

DVD Copy Control Authority (DVD-CCA)
http://www.dvdcca.org/

ElcomSoft Co. Ltd.
http://www.elcomsoft.ru/

Elcomsoft Executive Responds To Federal Charges Against Dmitry Sklyarov
http://elcomsoft.com/statement0829.html

Security workers: Copyright law stifles
http://news.com.com/2100-1001-272716.html?legacy=cnet

Law on Copyright and Neighboring Rights, Title II: Copyright,
Rospatent Russian Agency for Patent and Trademarks,
http://www.fips.ru/avpen/docs.htm

Norwegian authorities indict creator of DeCSS
http://europe.cnn.com/2002/TECH/industry/01/14/decss.writer.idg/index.html

Four years on, digital copyright law revs up
http://europe.cnn.com/2002/TECH/industry/02/18/copyright.law.idg/

Secure Digital Music Initiative
http://www.sdmi.org/

Hack SDMI Website / Secure Digital Music Initiative Public Challenge
http://censored.firehead.org:1984/hacksdmi.org/original-website/default.asp

Hack SDMI Website / Click-Through Agreement for the SDMI Public Challenge
http://censored.firehead.org:1984/hacksdmi.org/original-website/hacksClickThrough.asp

Electronic Frontier Foundation’s SDMI v. Felten Archive
http://www.eff.org/IP/DMCA/Felten_v_RIAA/

Frequently Asked Questions about Felten & USENIX v. RIAA Legal Case
http://www.eff.org/Legal/Cases/Felten_v_RIAA/faq_felten.html

Norwegian Research Center for Computers and Law, University of Oslo,
http://www.jus.uio.no/iri/english/index.html

Lov om opphavsrett til åndsverk [Åndsverkloven]
Act No. 2 of May 12, 1961, Relating to Copyright in Literary, Scientific and Artistic Works, etc., With Subsequent Amendments Up to June 30, 1995, [The Copyright Act]
http://www.unesco.org/culture/copy/copyright/norway/fr_sommaire.html

Act No. 40 of August 6, 1979
Provisional act relating to the photocopying etc. of protected works for use for educational purposes
http://www.unesco.org/culture/copy/copyright/norway/fr_sommaire.html

A Legal Perspective on the Norwegian DeCSS Case, Prof. Jon Bing (U. of Oslo, Norwegian Research Center for Computers and Law), Jan. 25, 2000
http://www.eff.org/IP/Video/DeCSS_prosecutions/Johansen_DeCSS_case/20000125_bing_johansen_case_summary.html

Endnotes

[1] Berne Convention for the Protection of Literary and Artistic Works
http://www.wipo.int/clea/docs/en/wo/wo001en.htm

[2] Russia - Accedes to the Berne Convention
http://www.ladas.com/BULLETINS/1995/0495Bulletin/Russia_JoinsBerne.html

[3] An Open Letter to the Digital Community
http://www.sdmi.org/pr/OL_Sept_6_2000.htm

[4] Click-Through Agreement for the SDMI Public Challenge
http://censored.firehead.org:1984/hacksdmi.org/original-website/hacksClickThrough.asp
http://www.cs.princeton.edu/sip/sdmi/clickthru.pdf

[5] "Reading Between the Lines: Lessons from the SDMI Challenge", Professor Edward Felten
http://www.usenix.org/publications/library/proceedings/sec01/craver.pdf

[6] 4th International Information Hiding Workshop
http://www.cert.org/IHW2001/

[7] RIAA/SDMI Legal Threat Letter (April 9, 2001)
http://www.eff.org/Legal/Cases/Felten_v_RIAA/20010409_riaa_sdmi_letter.html
http://cryptome.org/sdmi-attack.htm

[8] Statement of Professor Edward Felten at the Fourth International Information Hiding Workshop
http://www.eff.org/Legal/Cases/Felten_v_RIAA/20010426_felten_message.html
http://cryptome.org/sdmi-attack.htm

[9] Letter Alleging Criminal Conduct by Jon and Per Johansen, January 4, 2000,
http://www.eff.org/IP/Video/DeCSS_prosecutions/Johansen_DeCSS_case/20000104_dvdcca_no_prosecutor_letter.en.html

[10] Cornell Law School, Legal Informational Institute,
http://www.law.cornell.edu/topics/injunctions.html

[11] Federal Rules of Civil Procedure, Rule 65: Injunctions

[12] The American Heritage® Dictionary of the English Language, Fourth Edition
Copyright © 2000 by Houghton Mifflin Company