

THE DIGITAL MILLENNIUM COPYRIGHT ACT:
OVEREXTENSION OF COPYRIGHT PROTECTION AND
THE UNINTENDED CHILLING EFFECTS ON FAIR USE,
FREE SPEECH, AND INNOVATION

Derek J. Schaffner[†]

INTRODUCTION	145
I. IMPACT ON FAIR USE	149
II. IMPACT ON FREE SPEECH AND SCIENTIFIC RESEARCH	154
III. IMPACT ON INNOVATION AND COMPETITION	160
IV. UNRESOLVED ISSUES AND POTENTIAL SOLUTIONS	164
CONCLUSION.....	169

INTRODUCTION

The digital media revolution continues to evolve and challenge traditional notions of copyright protection. Media content companies and artists are very concerned as broadband access continues to become pervasive, leading to ubiquitous high-speed Internet access that permit gigabytes of copyrighted digital content to be shared across peer-to-peer networks without any remuneration to the artists or content companies who create such content. In response to this problem, Congress enlarged the reach of federal copyright law in 1998 with the passage of the Digital Millennium Copyright Act (DMCA)¹ to address the use of advanced technologies to bypass copyright protection mechanisms. In practice, however, the anti-circumvention provisions of the DMCA² have stifled a wide variety of activities, rather than prohibit copyright piracy. As a result, the DMCA has evolved into a serious threat to important public policy priorities including free speech, scientific research, fair use, and the promotion of competition and innovation.

The traditional goal of copyright protection is to promote the progress of science and useful arts by giving the author a constitutionally mandated short-term monopoly protecting the work against unauthorized

[†] J.D. Candidate, Cornell University Law School, 2005; M.S., University of Rochester, 1998; M.B.A., University at Buffalo, 1991; B.S., University at Buffalo, 1988. I would like to thank my wife, Justine, for her enduring support, patience, and encouragement.

¹ 17 U.S.C. § 1201 (2000).

² 17 U.S.C. § 1201(a)-(b) (2000).

infringement.³ The grant of exclusive rights of expression entails the limitation of expressive conduct by others, thus creating a First Amendment problem if the Constitution did not grant copyright protection. As a preemptive strike against unauthorized digital content sharing, copyright owners began to employ technological measures, often referred to as “digital rights management” (DRM) systems, to protect their digital works and control access to those works. The DMCA actually encourages copyright owners to utilize DRM systems by providing copyright owners with legal remedies against parties who circumvent those measures and against the suppliers of devices or technologies that facilitate such circumvention.⁴ However, DRM systems unduly shift the preexisting balance of interests toward copyright holders and away from copyright consumers and the public at large.

Theoretically, the use of DRM systems would allow a work with an expired copyright to remain protected forever by restricting consumer access through technology. For example, the DRM system used on DVDs enforces a “view-only” rule by using an encryption algorithm that is licensed to device manufacturers by the movie studios for a nominal fee on the condition that the algorithm is kept from the public.⁵ The reinforcement of such a system by the DMCA effectively gives copyright holders the power to control all downstream uses of content and therefore challenges the fair use doctrine of copyright. This, in turn, harms consumers by limiting their ability to enjoy legally acquired copyrighted content, raising First Amendment concerns.

The Supreme Court thought it settled the legitimacy of consumer copying when it held that home videotaping of copyrighted commercial television programs was fair use.⁶ Congress legitimized consumer copying when it recognized the right of consumers to make home recordings of music.⁷ However, the DMCA encouragement of DRM technologies casts considerable doubt on the validity of those previously settled activities as well as on the copying and file-sharing facilitated by the Internet and peer-to-peer networks.

Congress enacted the DMCA in response to two distinct pressures. First, the legislature was attempting to respond to the perceived need for the United States to implement obligations imposed by the 1996 World

³ See U.S. CONST. art. I, § 8, cl. 8.

⁴ 17 U.S.C. § 1201 (2000).

⁵ See *Universal City Studios, Inc. v. Corley*, 273 F.3d 429, 436-38 (2d Cir. 2001); see also Berkman Center for Internet & Society, Openlaw DVD/DeCSS Forum Frequently Asked Questions (FAQ) List, Section 3 – Technical Questions, at <http://cyber.law.harvard.edu/openlaw/DVD/dvd-discuss-faq.html> (on file with author).

⁶ See *Sony Corp. v. Universal City Studios, Inc.*, 464 U.S. 417 (1984).

⁷ See 17 U.S.C. § 1001 (2000).

Intellectual Property Organization Copyright Treaty.⁸ Second, the DMCA was a response to the growing concern from copyright owners regarding the pirating of digital content in a networked world. Section 1201 of the Act is comprised of two distinct prohibitions: a ban on acts of circumvention and a ban on the distribution of tools and technologies used for circumvention.⁹

The first prohibition, set out in Section 1201(a)(1), forbids the circumvention of DRM systems and other technological measures used by copyright owners to control access to their works.¹⁰ The ban on acts of circumvention applies even where the intent behind such acts is the otherwise legitimate decryption of a copyrighted work. For example, commercially released movies in VHS format allow consumers to fast forward through previews that preface the feature presentation. However, some movies released on DVDs restrict the consumer from making this choice and any efforts to circumvent this restriction would be unlawful under the DMCA.¹¹

The second prohibition, contained in sections 1201(a)(2) and 1201(b), make it illegal to manufacture, sell or distribute tools and technologies that make circumvention possible.¹² These provisions ban both technologies that defeat access controls, as well as technologies that defeat use-restrictions imposed by copyright owners, such as copy controls. Consequently, these provisions prevent technology vendors from taking steps to defeat the “copy-protection” now appearing on many music CDs. In addition, the music industry has begun deploying “copy-protected CDs” that curtail a consumer’s ability to make legitimate, personal copies of purchased music.¹³ Section 1201 also includes exceptions for certain limited classes of activities, including security testing, reverse engineering of software, encryption research, and law enforcement.¹⁴ However, these exceptions are too narrow to be of any real use to the intended constituencies.

Through my paper, I will attempt to demonstrate that the DMCA is not justifiable public policy because it grants too much power to the copyright holder and thus creates a chilling effect on fair use, free speech, future innovation, and competition. Part One will examine the ramifica-

⁸ WIPO Copyright Treaty, Dec. 20, 1996, available at <http://www.wipo.int/documents/en/diplconf/distrib/94dc.htm>.

⁹ 17 U.S.C. § 1201 (2000).

¹⁰ 17 U.S.C. § 1201(a)(1).

¹¹ Tom McNichol, *Fighting for Copy Rights*, WIREN (Jan. 2003), at <http://www.wired.com/wired/archive/11.01/start.html?pg=13>.

¹² *Id.*; 17 U.S.C. § 1201(a)(2), § 1201(b).

¹³ Gwendolyn Mariano, *Label Releases Copy-protected CD with Pride*, CNET NEWS (May 14, 2001), at <http://news.com.com/2100-1023-257621.html?legacy=cnet>.

¹⁴ 17 U.S.C. § 1201(d)-(g) (2000).

tions of the DMCA on the fair use doctrine. "Fair use," a fundamental element in American copyright law, allows a legitimate owner, without having to ask permission, to use copyrighted works in transformative other ways that do not unduly interfere with the copyright owner's market for a work.¹⁵ Fair uses include personal, noncommercial uses as well as activities undertaken for purposes such as criticism, comment, news reporting, teaching, scholarship, and research.¹⁶ While enforcement of copyright protection is an important policy goal, the DMCA overextends this protection. Copyright owners can effectively eliminate fair use by utilizing DRM systems sanctioned under the DMCA and litigating against anyone who tampers with those measures. Thus, re-writing the copyright fundamentals developed by Congress and courts over more than a century.

In Part Two, I will explore the impact that the DMCA has on free speech and scientific research. For example, Internet Service Providers (ISPs) have begun to censor discussions of copy-protection systems, programmers have removed computer security programs from their websites, and security experts have stopped publishing details of their research on security protocols.¹⁷ These developments may result in weakened computer security for all users as researchers consciously avoid certain activities for fear that they may become legally liable under the DMCA. Ironically, this could have an impact on digital copyright owners who rely on encryption technology to protect their work.

Part Three will examine the impact of the DMCA on innovation and competition. Rather than battle piracy, copyright holders are using the DMCA to deter marketplace competitors. For example, copyright holders are using the DMCA to hinder the efforts of legitimate competitors to create interoperable products, thus resulting in increased costs for the consumer. Several computer game publishers have invoked the DMCA to prohibit others from using reverse engineering to create versions of their games that would run on alternative operating systems.¹⁸

Experience with the "anti-circumvention" provisions of the DMCA¹⁹ demonstrates that the statute reaches too far, chilling a wide variety of legitimate activities in ways Congress did not intend. As technological protection measures wrap an increasing number of copyright works, it is likely that copyright holders will apply the DMCA's anti-

¹⁵ 17 U.S.C. § 107 (2000).

¹⁶ *Id.*

¹⁷ See generally Niels Ferguson, *Censorship in Action: Why I Don't Publish My HDCP Results*, at <http://cyber.law.harvard.edu/archive/dvd-discuss/msg14730.html> (posted Aug. 16, 2001).

¹⁸ See *Sony Computer Entm't Am., Inc. v. GameMasters*, 87 F. Supp. 2d 976 (N.D. Cal. 1999).

¹⁹ 17 U.S.C. § 1201(a)(1) (2000).

circumvention provisions in further unforeseen contexts hindering the legitimate activities of innovators, researchers, the press, and the public at large.

Part Four will examine the most critical unresolved issues facing the DMCA, such as the emergence of digital video recorders, and propose alternative solutions to ensure the preservation of rights of copyright owners while minimizing the negative effects of the DMCA.

I. IMPACT ON FAIR USE

Copyright holders using Digital Rights Management (DRM) technologies may threaten a wide range of consumers seeking greater control over media they rightfully own, as the Digital Millennium Copyright Act (DMCA) makes unauthorized circumvention of access and copy controls subject to criminal prosecution.²⁰ The force of law that encourages the use of DRM technologies could lead to copyright holders developing a new intellectual property regime based entirely in computer code, abandoning traditional copyright measures for digital works.²¹ Such a regime is problematic because it could hinder the ability to access material that has fallen out of copyright or prohibit the acceptable copying of copyrighted material under a “fair use” rationale.

The fair use doctrine essentially allows the reproduction of copyrighted material for certain uses deemed non-infringing such as “comment, news reporting, teaching (including multiple copies for classroom use), scholarship, or research.”²² To determine whether a particular use is covered under a fair use exception, the court will analyze four factors:

- 1) the purpose and character of the use, including whether such use is of a commercial nature or is for non-profit 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.²³

Fair use, a critical element of copyright law, stands for the principle that the public, is entitled to use copyrighted works in transformative ways or other ways that do not interfere with the copyright holder’s mar-

²⁰ See 17 U.S.C. § 1201(a)(1)(A), § 1203(a) (2000), § 1204(a) (2000).

²¹ See generally Dan L. Burk, *Anti-Circumvention Misuse*, 50 UCLA L. REV. 1095 (2003).

²² 17 U.S.C. § 107 (2000).

²³ *Id.*

ket for a work.²⁴ Fair uses include personal, noncommercial uses, such as using a VCR to record a television program for later viewing.²⁵ While the fair use doctrine has been successfully applied to some technology-assisted copying,²⁶ this defense has failed at other times,²⁷ creating an unpredictable environment for the application of fair use. For example, Sony has invoked the fair use doctrine as both a sword and shield by successfully using the fair use defense to insulate its Betamax VCR product²⁸ and later invoking the DMCA to threaten hobbyists who utilized reverse-engineering techniques to build additional software functionality for Sony's Aibo robot dog.²⁹ However, the fair use defense has also been successfully used against Sony by the creators of software that permits Playstation games to be played on personal computers.³⁰

These examples illustrate the imprecise application of fair use when applied to DRM systems and illustrate that fair use cannot be defined with precision. The statutory four factor test codified in 17 U.S.C. § 107 includes concepts that are not easily expressed in precise business rules such as "effect on the market" and "commercial/noncommercial."³¹ Such ambiguity is by design because it is vital that the fair use doctrine continue to evolve as new technologies develop. Since courts typically have the first opportunity to apply copyright law to new technology, this doctrine must be flexible to spare copyright owners and technologists from having to lobby the Congress every time a new piece of technology is developed. The fair use doctrine, therefore, plays a critical role in allowing innovation to flourish while Congress has time to evaluate new technologies and develop any appropriate legislative solutions.

A fair use situation typically arises when one party makes use of another's work that he believes to be "fair" under the current circumstances.³² If the copyright holder disagrees with the alleged fair use of his work, he can sue for copyright infringement and ask the court to rule

²⁴ See *Sony Corp. v. Universal City Studios, Inc.*, 464 U.S. 417, 477-82 (1984) (Blackmun, J., dissenting).

²⁵ See *id.* at 499 (using a device, capable of significant non-infringing uses as well as infringing uses, does not infringe copyright).

²⁶ *Id.*

²⁷ See *A&M Records, Inc. v. Napster, Inc.*, 239 F.3d 1004 (9th Cir. 2001) (copying of digital music files by a person who owns the recording on a compact disc is infringing activity not covered by fair use).

²⁸ *Sony Corp.*, 464 U.S. 417.

²⁹ Will Knight, *Aibo Custom Code Pulled From Website*, NEW SCIENTIST (Oct. 30, 2001), available at <http://www.newscientist.com/news/news.jsp?id99991495>.

³⁰ See *Sony Computer Entm't, Inc. v. Connectix Corp.*, 203 F.3d 596 (using plaintiff's software during the course of reverse engineering is a protected fair use, necessary to permit defendant to make its non-infringing system function with plaintiff's system).

³¹ 17 U.S.C. § 107 (2000).

³² See generally H.R. REP. NO. 94-1476, at 65 (1976).

on the use.³³ However, this process is bypassed if the copyrighted work is protected by a DRM system because the DMCA prohibits the circumvention of any DRM access or control system.³⁴ Therefore, the DMCA will force the fair use doctrine to be limited to those uses which the courts have previously affirmed. As a result, the development of any new uses will be hindered because the alleged infringer will not be allowed to legally bypass the DRM system to access the underlying work. The ambiguity of the fair use doctrine cannot flourish under such a strict interpretation of DRM system circumvention codified in the DMCA. To allow the fair use doctrine to operate as intended, DRM systems and the DMCA must find a way to reflect the ambiguity of the doctrine and embrace unrealized uses of copyrighted material.

Digital Rights Management systems may be viewed as a form of “technological self-help” that copyright holders can employ as a “hedge against content infringement” and thus, avoid traditional forms of copyright protection.³⁵ DRM technology allows the content owner to select a customized level of protection making the regulation of copyright content via legal sanctions less attractive.³⁶ When the DMCA reinforces the use of such technological measures, content owners achieve a level of control unattainable under a traditional copyright system.³⁷ Given the provisions of DMCA, it seems unlikely that digital content producers who favor strong technological protection to fend off digital piracy would endorse a system that offers fair use flexibility.

A copyright represents a bargain between the public and the copyright owner whereby the public grants certain limited exclusive rights to the copyright owner in order to create an incentive for the production of creative works.³⁸ Assuming that a copyright owner would favor technological self-help over traditional legal protection, the equilibrium of the aforementioned bargain is thus askew since the public has lost its ability to use DRM-protected works under a fair use scenario.³⁹

Proponents of technology controls often justify such measures as a means to combat digital piracy.⁴⁰ Unfortunately, the DMCA has given digital content providers more control over copyrighted material to com-

³³ See *id.*

³⁴ 17 U.S.C. § 1201 (2000).

³⁵ Burk, *supra* note 21, at 1097.

³⁶ See *id.* at 1100-01.

³⁷ See Glynn S. Lunney, Jr., *The Death of Copyright: Digital Technology, Private Copying, and the Digital Millennium Copyright Act*, 87 VA. L. REV. 813 (2001).

³⁸ See U.S. CONST. art. I, § 8, cl. 8.

³⁹ See generally Kenneth W. Dam, *Self-Help in the Digital Jungle*, 28 J. LEGAL STUD. 393 (1999) (defines self-help systems and argues that they can develop to accommodate fair users and also work to deter unauthorized copying).

⁴⁰ See generally John Borland, *Hacker Cracks Microsoft Anti-piracy Software*, CNET News (Oct. 19, 2001), at <http://news.com.com/2100-1023-274721.html?legacy=cnet> (news re-

bat digital piracy at the expense of the public losing its fair use power. Digital content producers argue that piracy must be stopped; otherwise, the economic incentive to create additional works will disappear if a copyright holder is not able to realize a return on his investment.⁴¹ However, the software industry has thrived for years operating with minimal technological controls; Microsoft has not been harmed by publishing early versions of DOS and Windows without any copy protection.⁴²

Nonetheless, if the fair use doctrine is allowed to erode in favor of DRM systems, there will be several negative impacts. As greater amounts of content are delivered in digital form, there could be a possible reduction in expression to the extent that technological self-help interferes with access to the underlying works. This could reduce several fair uses of copyrighted material such as review, commentary, parody, and scholarly use.⁴³ The erosion of fair use could also have an impact on innovation and competition. For example, if DRM systems restrict content access to the exclusion of complementary products, a reduction in innovation for interoperable products could occur as DRM systems eliminate the incentives to create such products. Likewise, DRM systems could be used to reduce competition by preventing others from engaging in legitimate reverse engineering of competitive products. There are social costs as well, such as the erosion of privacy if DRM technologies compromise user anonymity. Libraries and archives may also be affected to the extent that DRM systems make the archiving of copyrighted content more difficult.

The collision between fair use and the DMCA has been highlighted with the introduction of “copy-protected” compact discs.⁴⁴ The recording industry is aggressively incorporating DRM technology on new music releases.⁴⁵ Irrespective of the impact these systems will have on online music swapping, they certainly will interfere with the fair use expectations of consumers. Many of these systems prohibit consumers from creating MP3s, a digital format that allows music files to be easily duplicated, and thus prevent consumers from “space shifting” legally

port on a software program that successfully cracked part of Microsoft’s anti-piracy technology).

⁴¹ See Alfred Hermida, *Real Boss Tackles Online Piracy*, BBC News (Feb. 18, 2003), available at <http://news.bbc.co.uk/1/hi/technology/2758177.stm>.

⁴² See generally Microsoft Investor Relations website, *Microsoft fiscal year financial history*, at <http://www.microsoft.com/msft/download/financialhistoryFY.xls> (on file with author).

⁴³ 17 U.S.C. § 107.

⁴⁴ See Gwendolyn Mariano, *Copy-Protected CDs Slide into Stores*, CNET News (Feb. 12, 2002), at <http://news.com.com/2100-1023-835841.html>.

⁴⁵ *Id.*

purchased music to their personal computers.⁴⁶ For example, copy-protected discs will disappoint consumers who have purchased MP3 players, despite the fact that making an MP3 copy of a compact disc for personal use appears to be protected under copyright law.⁴⁷

Over two-hundred million copy-protected compact discs are in circulation,⁴⁸ but the technology has not always worked as intended. In 2003, a Princeton Ph.D. student explained how he disabled a new kind of copy-protection technology distributed as part of a new compact disc by holding down the “Shift” key on the keyboard when attempting to play the disc on his personal computer.⁴⁹ A strict reading of the DMCA would suggest that this simple act could be viewed as the circumvention of a copy-protection system.⁵⁰

As more content is produced and delivered in a digital format, the future ability to make legitimate fair uses of these works is dependant upon the availability of tools to bypass these digital protection systems. However, the DMCA’s anti-circumvention provisions prohibit the distribution and creation of such tools.⁵¹ While some might be tempted to use such tools to promote piracy, the traditional solution to copyright piracy has been prosecution under the legal regime, not a wholesale ban on tools that may potentially enable fair use.⁵²

Unfortunately, some fair use tools have already been removed from the market. In *Universal City Studios, Inc. v. Reimerdes*, eight major motion picture companies brought a DMCA suit against several defendants, including Eric Coley who published a magazine and maintained an affiliated website, seeking to block the defendants from publishing links to a software program which defeated the encryption used on DVD movies.⁵³ The website, which was not involved in the development of the program, made the software tool available during its ongoing coverage of the DMCA controversy.⁵⁴ The district court permanently barred the

⁴⁶ See John Borland, *Right Issue Dogs CD Protection*, CNET NEWS (Jan. 13, 2004), at <http://news.com.com/2100-1027-5139762.html>.

⁴⁷ See *Recording Indus. Ass’n of Am. v. Diamond Multimedia Sys.*, 180 F.3d 1072, 1079 (8th Cir. 1999) (holding that ripping MP3’s from legally-acquired compact discs and copying them from a personal computer to a portable MP3 player facilitates personal use under the Audio Home Recording Act of 1992 (Act), 17 U.S.C.S. § 1001, and that such “space shifting” is a legitimate personal use analogous to “time shifting” in *Sony Corp. v. Universal City Studios*, 464 U.S. 417, 455, (1984)).

⁴⁸ Borland, *supra* note 46.

⁴⁹ See John Borland, *Shift Key Breaks CD Copy Locks*, CNET NEWS (Oct. 7, 2003), at <http://news.com.com/2100-1025-5087875.html>.

⁵⁰ See 17 U.S.C. § 1201(a) (2000).

⁵¹ See 17 U.S.C. § 1201(b)(1)(A) (2000).

⁵² See David Nimmer, *A Riff on Fair Use in the Digital Millennium Copyright Act*, 148 U. PA. L. REV. 673, 683-84 (2000).

⁵³ 82 F. Supp. 2d 211, 213-15 (S.D.N.Y. 2000).

⁵⁴ *Id.* at 214-15.

magazine from publishing, or even linking to, the code, and the Second Circuit Court of Appeals affirmed.⁵⁵

Despite the ruling in *Reimerdes*, there are many legitimate reasons to copy DVDs. Once the video is transferred to a personal computer, many fair uses become possible. For example, film makers could take public domain content from another region and create a digital derivative work; consumers could fast-forward through the commercials that preface many films. Without the tools necessary to copy DVDs, however, these fair uses become impossible.

While it may be too early to draw final conclusions, it is plain that DRM technologies, backed by the force of the DMCA, pose a serious potential threat to fair use. While technical refinements may address or minimize some of the social costs that stem from an erosion of fair use, it is unlikely that they will entirely resolve the tension. The issue then becomes one of trade-offs, not reconciliation. With its passage of the DMCA, Congress has essentially delegated copyright law for digital content to copyright owners and DRM vendors. Such a regime is not likely to produce beneficial results for the public.

II. IMPACT ON FREE SPEECH AND SCIENTIFIC RESEARCH

A number of copyright owners are using the DMCA to stifle free speech and legitimate scientific research. In response to DMCA liability fears, online service providers and bulletin board operators have begun to censor discussions of copy-protection systems, programmers have removed security programs from their websites, and academics have stopped publishing the details of their research on security protocols.⁵⁶ Foreign scientists are increasingly uneasy about traveling to the United States out of fear of possible DMCA liability, and certain technical conferences have begun to relocate overseas.⁵⁷ These developments may ultimately result in weakened security for all computer users as security researchers shy away from research that might violate the DMCA.

The ubiquity of the Internet and its evolution as a communications tool accessible by the masses raise new questions regarding the constitutional right to Freedom of Speech in cyberspace. The First Amendment to the U.S. Constitution states that "Congress shall make no law . . . abridging the freedom of speech, or of the press."⁵⁸ Before imposing any content-based restriction of speech, the First Amendment and interpretative case law require that the federal government meet a high level of

⁵⁵ See *Universal City Studios, Inc. v. Reimerdes*, 111 F. Supp. 2d 294, 346, *aff'd sub nom* *Universal City Studios, Inc. v. Corley*, 273 F.3d 429, 434-35 (2d Cir. 2001).

⁵⁶ See Ferguson, at <http://cyber.law.harvard.edu/archive/dvd-discuss/msg14730.html>.

⁵⁷ See discussion *infra* pp. 18-19.

⁵⁸ U.S. CONST. amend. I.

scrutiny.⁵⁹ In the first Supreme Court case dealing with communication on the Internet, *Reno v. ACLU*, the Court affirmed that online speech deserves as much protection as off-line speech.⁶⁰

However, powerful media entities have successfully invoked the DMCA as a sword to chill speech without having to meet any level of scrutiny, much less the heightened one accorded off-line speech. One of the earliest challenges to online freedom of speech foreclosed by the DMCA occurred in *Universal City Studios, Inc. v. Corley*, where eight major movie studios sought to enjoin a web publisher from providing links to sites carrying a piece of software that the studios perceived to be a threat to the movie industry.⁶¹ Eric Corley, one of the defendants in the case, published a magazine “2600: The Hacker Quarterly” and operated an auxiliary website entitled “2600.com.”⁶² In January 2000, the movie studios sued Corley for publishing an article on his website which explained that a software program called DeCSS could be used to copy DVDs.⁶³ The studios objected to hypertext links provided in the article that would take the reader to a website where the controversial code could be downloaded.⁶⁴

DeCSS was developed by Norwegian teenager Jon Johansen and immediately drew a great deal of interest from the Linux open source community.⁶⁵ Linux is a fledging operating system that is freely distributed, and its source code may be modified by anyone who chooses to work on it, provided that others can view the underlying programming code.⁶⁶ Movies released in the DVD format are protected by a security system called the Contents Scramble System (CSS).⁶⁷ Under the CSS scheme, movie data embedded in the DVD disks is encrypted and may only be decrypted and played back for viewing on an authorized DVD player or computer hard drive that has a licensed CSS key.⁶⁸ The Linux operating system was developed via a global volunteer network, resulting in the lack of central ownership and thus prohibiting the ability to license

⁵⁹ See generally *Va. State Bd. of Pharmacy v. Va. Citizens Consumer Council*, 425 U.S. 748 (1976).

⁶⁰ See *Reno v. ACLU*, 521 U.S. 844, 885 (1997).

⁶¹ See *Universal City Studios, Inc. v. Corley*, 273 F.3d 429 (2d Cir. 2001).

⁶² Carl S. Kaplan, *Norwegian Teenager Appears at Hacker Trial He Sparked*, N.Y. TIMES CYBER LAW JOURNAL (July 20, 2000), available at <http://archive.nytimes.com/library/tech/00/07/cyber/cyberlaw/21law.html>.

⁶³ *Id.*

⁶⁴ *Id.*

⁶⁵ *Id.*

⁶⁶ Some companies distribute Linux as part of a commercial package with Linux-compatible utilities. An example of one such company is Red Hat (<http://www.redhat.com>).

⁶⁷ Berkman Center for Internet & Society, Openlaw DVD/DeCSS Forum Frequently Asked Questions (FAQ) List, *supra* note 5.

⁶⁸ *Id.*

CSS for DVD playback.⁶⁹ In an effort to develop an open-source software player that would allow people to play their lawfully purchased DVDs on computers running the Linux operating system, Johansen created DeCSS to allow Linux users the same functionality afforded non-Linux users.⁷⁰

Regardless of any benefits accruing to Linux users, the New York District Court and the 2nd Circuit Court of Appeals viewed Johansen's program as a tool to infringe the copyrights of DVD publishers.⁷¹ District Court Judge Kaplan sided with the movie studios and ordered Corley to remove all links to DeCSS from his website.⁷² In his opinion, Kaplan held that DeCSS circumvented the CSS access-control scheme, thereby violating the "anti-circumvention" provision of the DMCA.⁷³ Additionally, the court found that Corley violated the "anti-trafficking" provision of the DMCA by providing links to sites from which users could download DeCSS.⁷⁴ Although Corley did not have an actual copy of DeCSS available for download at his website, the court's injunction prohibiting him from providing DeCSS links violated his freedom of speech without passing the traditional high level of scrutiny test required to justify a content-based speech restriction.⁷⁵ The New York Times, the San Jose Mercury News, the Village Voice, and several other mainstream news outlets also reported the issue and linked to DeCSS.⁷⁶

In an attempt to justify its position, the Court of Appeals held that the code used was protected speech, but the functional aspect of the speech was targeted and thus survived intermediate scrutiny.⁷⁷ In the court's view, the capacity of DeCSS to accomplish unauthorized and unlawful access necessarily limited the scope of First Amendment protection available.⁷⁸ The court stated that DeCSS had both speech and non-speech components, and the linking injunction targeted only the non-speech component.⁷⁹ Nonetheless, the injunction prohibited Corley from sharing information he felt was newsworthy, and thus his cyberspace freedom of speech was violated. This decision was in stark contrast to the Supreme Court's ruling in *Reno v. ACLU*.⁸⁰

⁶⁹ See generally The Linux Home Page, at <http://www.linux.org>.

⁷⁰ Kaplan, *supra* note 62.

⁷¹ *Reimerdes*, 111 F. Supp. 2d at 346.

⁷² *Id.* at 347.

⁷³ *Id.* at 346.

⁷⁴ *Id.*

⁷⁵ See *Va. State Bd. of Pharmacy*, 425 U.S. at 748.

⁷⁶ Carl S. Kaplan, *Is Linking Illegal?*, N.Y. TIMES CYBER LAW JOURNAL (June 16, 2000), available at <http://archive.nytimes.com/library/tech/00/06/cyber/cyberlaw/16law.html>.

⁷⁷ *Corley*, 273 F.3d at 442.

⁷⁸ *Id.* at 453.

⁷⁹ *Id.* at 456-58.

⁸⁰ 520 U.S. 1113 (1997).

Another crucial test of the constitutional limits of the DMCA occurred in *United States v. Elcom Ltd.*⁸¹ This case was launched in 2001 when a Russian software company employee was arrested during a conference in Las Vegas after delivering a presentation that described his company's software.⁸² The product was designed to unlock protections on Adobe Systems' eBooks that bound digital content to only one device.⁸³ Although the Russian company faced charges of violating the DMCA for its actions related to the design and marketing of software that could bypass eBook copyright protections, this program allowed users to enjoy legally-purchased eBook content on more than one device.⁸⁴ For example, the Adobe technology prohibited a user from making a copy of legally-acquired content for use on his laptop if the original version resided on his desktop computer.⁸⁵

In its defense, ElcomSoft claimed that Section 1201(b) of the DMCA⁸⁶ was unconstitutionally vague and that the statute violated the First Amendment because it constituted a content-based restriction on speech not sufficiently tailored to serve a compelling state interest.⁸⁷ The Russian company also asserted that Section 1201(b) was unconstitutional because it impermissibly infringed the First Amendment rights of third parties to engage in fair use and because it was too vague in describing what speech it prohibits.⁸⁸ Finally, the company argued that Congress exceeded its constitutional power in enacting the DMCA.⁸⁹

The court held that Section 1201(b) was not unconstitutionally vague because it allowed a person to conform his or her conduct to a comprehensible standard.⁹⁰ The court also held that the governmental interests in enacting the DMCA were both legitimate and substantial and did not burden considerably more speech than was necessary to achieve those interests.⁹¹ The court finally held that the DMCA was not unconstitutionally vague on its face and that Congress did not exceed its power in enacting it.⁹² While the jury found that ElcomSoft's program was

⁸¹ 203 F. Supp. 2d 1111 (N.D. Cal. 2002).

⁸² Jeff German, *Russian Software Developer Arrested in Vegas*, LAS VEGAS SUN (July 18, 2001), available at <http://www.lasvegassun.com/sunbin/stories/lv-crime/2001/jul/18/512096646.html>.

⁸³ *Id.*

⁸⁴ *Id.*; Joanna Glasner, *Verdict Seen As Blow to DMCA*, WIRED (Dec. 18, 2002), available at <http://www.wired.com/news/business/0,1367,56898,00.html>.

⁸⁵ *Elcom*, 203 F. Supp. 2d at 1117-18.

⁸⁶ 17 U.S.C. § 1201(b) (2000).

⁸⁷ *Elcom*, 203 F. Supp. 2d at 1122.

⁸⁸ *Id.* at 1134.

⁸⁹ *Id.* at 1137.

⁹⁰ *Id.* at 1136-37.

⁹¹ *Id.* at 1132.

⁹² *Id.* at 1137, 1141-42.

illegal, the jury acquitted the company of all charges after determining that the company did not willfully intend to violate the DMCA.⁹³

Since the arrest of the ElcomSoft employee, foreign scientists have expressed concerns about traveling to the United States.⁹⁴ Some have even advocated boycotting conferences held in the U.S., and a number of conference bodies have decided to move their conferences to non-U.S. locations.⁹⁵ In fact, Russia has issued a travel warning to Russian programmers traveling to the U.S.⁹⁶ Highly respected British Linux programmer Alan Cox resigned from the USENIX committee of the Advanced Computing Systems Association, the committee that organizes many of the U.S. computing conferences.⁹⁷ Cox referred to concerns about traveling to the U.S. as one of the reasons for his resignation and urged USENIX to hold its annual conference offshore.⁹⁸

Section 1201 of the DMCA⁹⁹ is also being used to stifle legitimate scientific research. Ironically, computer security research is a major area where the oppressive impact of the DMCA is most felt. In response to concerns from technologists that earlier drafts of the DMCA could have the potential to outlaw the necessary research and testing required to build computer security products,¹⁰⁰ Congress included two narrow exceptions in the DMCA for encryption research and security testing.¹⁰¹ However, these exceptions are too narrow: computer scientists, entangled in litigation, divert from security research while trying to comply with the DMCA.¹⁰² These developments will ultimately result in weakened security for all computer users as security researchers shy away from useful work that might violate the DMCA. In fact, Richard Clarke, the head of the White House Office of Cyberspace Security, recently called

⁹³ Lisa M. Bowman, *ElcomSoft Verdict: Not Guilty*, CNET NEWS (Dec. 17, 2002), at <http://news.com.com/2100-1023-978176.html>.

⁹⁴ Will Knight, *Computer Scientists Boycott US over Digital Copyright Law*, NEW SCIENTIST, July 23, 2001.

⁹⁵ *Id.*

⁹⁶ Jennifer Lee, *Travel Advisory for Russian Programmers*, N.Y. TIMES, Sept. 10, 2001, at C4.

⁹⁷ *Alan Cox Resigns from Usenix ALS Committee, Cites DMCA*, NEWSFORGE (July 20, 2001) at <http://www.newsforge.com/article.pl?sid=01/07/20/1228200>.

⁹⁸ *Id.*

⁹⁹ 17 U.S.C. § 1201 (2000).

¹⁰⁰ See Jonathan Band, *Congress Unknowingly Undermines Cyber-security*, SILICON VALLEY NEWS (Dec. 16, 2002), available at <http://www.siliconvalley.com/mld/siliconvalley/4750224.htm>.

¹⁰¹ See 17 U.S.C. § 1201(g) (2000).

¹⁰² See Professor Ross Anderson, Cambridge University, Declaration in *Felten v. RIAA* (Oct. 22, 2001) (describing ways in which the DMCA is suppressing research into security weaknesses in SDMI watermarking technology), available at http://www.eff.org/IP/DMCA/Felten_v_RIAA/20011022_anderson_decl.pdf.

for an amendment to the DMCA because of its “chilling effect on vulnerability research.”¹⁰³

The threat to scientific research has been highlighted by the efforts of the Recording Industry Association of America (RIAA) and the Secure Digital Music Initiative (SDMI) Foundation to utilize the DMCA to suppress academic research. SDMI is a multi-industry group, formed largely at the instigation of the RIAA to develop technical standards for “watermarks” and compliant devices, whose charter is “to develop open technology specifications that protect the playing, storing, and distributing of digital music such that a new market for digital music may emerge.”¹⁰⁴ In September 2000, SDMI issued a public challenge to encourage technologists to attempt to defeat certain digital rights management (DRM) watermarking technologies intended to protect digital music.¹⁰⁵ Professor Edward Felten of Princeton University’s Computer Science Department and a team of researchers from Princeton, Rice, and Xerox subsequently succeeded in removing the DRM technology.¹⁰⁶

Felten and his team documented their findings in an academic paper, including weaknesses of the SDMI watermarking system, and planned to present their findings at an academic conference.¹⁰⁷ Executives at SDMI and the RIAA attempted to persuade Felten to remove certain sections of the paper, especially those critical of the SDMI DRM system.¹⁰⁸ Felten and his team refused because they felt these details were necessary to support their scientific findings.¹⁰⁹ SDMI and the RIAA then invoked the DMCA and asserted that any presentation of the paper at the academic conference would subject the researchers and their institutions to liability and threatened legal action unless the research team withdrew the paper.¹¹⁰ As a direct result of the DMCA threat, Felten and his team grudgingly withdrew their paper from the conference, preventing other technology researchers from learning about the weaknesses of the SDMI watermarking system.¹¹¹ Thus, the DMCA had a chilling effect on the sharing of scientific research.

The use of the DMCA to suppress the sharing of scientific research in situations like those found in *Elcom*¹¹² and Professor Felten’s paper is

¹⁰³ Band, *supra* note 100.

¹⁰⁴ <http://www.sdmi.org>.

¹⁰⁵ See Thomas C. Greene, *Felten Spills the SMDI Beans*, THE REGISTER (Aug. 16, 2001), at <http://www.theregister.co.uk/content/6/21086.html>.

¹⁰⁶ See *id.*

¹⁰⁷ See Pamela Samuelson, *Anticircumvention Rules: Threat to Science*, SCIENCE, Sept. 14, 2001, at 2028.

¹⁰⁸ See *id.*

¹⁰⁹ *Id.*

¹¹⁰ *Id.*

¹¹¹ See *id.*

¹¹² *Elcom*, 203 F. Supp. 2d at 1111.

forcing many researchers to reconsider publication of their results. Such restrictions could have a deleterious effect on the computer security industry in the United States, as foreign researchers avoid publication and conference participation for fear of being prosecuted under the DMCA. A Dutch cryptographer recently refused to publish news of an alleged flaw in some technology designed to protect digital video developed by Intel.¹¹³ The researcher cited fear of prosecution under the DMCA as the basis for refusing to divulge specific details regarding the flaw, stating: "I have decided to censor myself and not publish this paper for fear of prosecution and/or liability under the U.S. DMCA law."¹¹⁴

The DMCA pushes the limits of constitutionality when copyright holders are allowed to use the Act as a sword to suppress speech and the free exchange of ideas. This is especially notable in the computer security industry, which could reap tremendous benefits if the anti-circumvention measures of the DMCA were less restrictive and allowed researchers the opportunity to benefit from the work of others. As a leader in information technology products, the United States cannot afford to have its academic pipeline of research chilled by the overly oppressive provisions of the DMCA.

III. IMPACT ON INNOVATION AND COMPETITION

Copyright holders may use the DMCA to stifle innovation and reduce competition in the marketplace by hindering the efforts of legitimate competitors attempting to develop interoperable products. Such use of the Act will lead to DMCA-endorsed monopolies, which will ultimately leave consumers with fewer choices and higher prices. For example, Blizzard Entertainment and parent company Vivendi-Universal have recently invoked the DMCA in an effort to intimidate the developers of a software program derived from legitimate reverse engineering.¹¹⁵ The company alleges that the software, which allows users to compete against each other in Blizzard video games over the Internet, violates both the DMCA's prohibition on circumventing access control measures and Blizzard's end user license agreements (EULAs).¹¹⁶ The verbose EULAs, which users of such games must accept, contain sweeping restrictions on reverse engineering, decompilation, and disassembly.¹¹⁷ Here, the company has used the DMCA to deter a marketplace competitor rather than to battle piracy.

¹¹³ See Lisa M. Bowman, *Researchers Weigh Publication, Prosecution*, CNET NEWS (Aug. 15, 2001), at <http://news.com.com/2100-1023-271712.html?legacy=cnet>.

¹¹⁴ See *id.*

¹¹⁵ See *Blizzard Entertainment v. Internet Gateway, Inc.*, No. 4:02CV00498CAS (E.D. Mo. filed Apr. 5, 2002).

¹¹⁶ *Id.*

¹¹⁷ *Id.*

On its face, the DMCA's prohibition would prevent reverse engineering of measures that control access to a copyrighted work since circumvention is generally required for reverse engineering. The DMCA contains a limited exception to the ban on circumvention, which permits reverse engineering of the technology by specific classes for limited purposes.¹¹⁸ The exception allows reverse engineering of computer programs if the reverse engineer lawfully obtains the program, seeks permission from the copyright owner, uses the results of his efforts only to create an interoperable computer program, and does not publish the results.¹¹⁹ However, the resulting program must only interoperate with the reverse engineered software and cannot interoperate with the technologically-protected content such as movies, books, and video games.¹²⁰ As a result, reverse engineers must carefully consider their planned work because this exception is far too narrow to be useful for many reverse engineering needs.

It is fair to say that eliminating all competition from an industry is not what Congress intended when it promulgated the DMCA, but that is precisely the effect this legislation is having on the laser printer toner aftermarket. Lexmark, the second-largest printer vendor in the U.S., has long tried to eliminate aftermarket laser printer toner vendors that offer toner cartridges at prices below Lexmark's.¹²¹ It is well known within that industry that toner and ink cartridge sales represent the most profitable items for such manufacturers.¹²²

Lexmark devised a clever way to force buyers of its printers to use only the company's brand of replacement toner cartridges. A Lexmark printer will run only if the toner cartridge has a computer chip that sends an authentication sequence to the printer that identifies the cartridge as manufactured by Lexmark.¹²³ If a user installs a less-expensive toner cartridge from another manufacturer, the machine will not function. In December 2002, Lexmark invoked the DMCA as a new weapon in its arsenal and brought suit against printer microchip manufacturer Static Control Components.¹²⁴ Lexmark sought to prohibit Static from selling chips it claimed were "technology" which "circumvented" certain "authentication routines" between Lexmark toner cartridges and printers.¹²⁵

¹¹⁸ See 17 U.S.C. § 1201(f) (2000).

¹¹⁹ See *id.*

¹²⁰ See *id.*

¹²¹ See Declan McCullagh, *Lexmark Invokes DMCA in Toner Suit*, CNET NEWS (Jan. 8, 2003), at <http://news.com/2100-1023-979791.html>.

¹²² See Peter Judge, *HP Admits It's the Ink That Counts*, ZD NET UK (Mar. 7, 2002), at <http://news.zdnet.co.uk/hardware/0,39020351,2106094,00.htm>.

¹²³ See McCullagh, *supra* note 121.

¹²⁴ *Lexmark Int'l, Inc. v. Static Control Components, Inc.*, No. 02-571-K5F (E.D. Ky. filed Dec. 30, 2002).

¹²⁵ *Id.*

Lexmark added these authentication routines explicitly to hinder aftermarket toner vendors, but the defendant had reverse-engineered these software measures and marketed “Smartek” chips that enabled aftermarket cartridges to work in Lexmark printers.¹²⁶ Though the Ninth Circuit Court previously supported the use of reverse engineering for intermediate copying of software code,¹²⁷ the District Court granted Lexmark a preliminary injunction prohibiting Static Control from the manufacture and sale of these chips.¹²⁸ However, the Sixth Circuit recently overturned the decision to grant Lexmark an injunction and remanded the case for further proceedings.¹²⁹

Even just the threat of litigation for DMCA violations has been enough to stifle innovation. Apple Computer invoked the Act in August 2002 to prevent customers from burning DVDs on external drives.¹³⁰ The main issue involved Apple’s iDVD application, which allows users to burn DVDs only on internal drives manufactured by the company.¹³¹ The program does not permit users to burn content to external drives manufactured by third parties.¹³² This has essentially stranded Apple owners with older computers or laptops because they cannot use iDVD to save their work. Apple is highly motivated to sell new hardware since equipment sales comprise eighty-five to ninety percent of the company’s quarterly revenue,¹³³ and thus has locked customers into a proprietary hardware upgrade.

As a result of this backwards incompatibility, Other World Computing began bundling a product called DVD Enabler with an external drive that modified iDVD so the application would save completed DVDs to a FireWire-connected drive.¹³⁴ Apple subsequently threatened Other World with legal action, asserting that the company’s product was a violation of the DMCA.¹³⁵ Other World responded by withdrawing DVD Enabler immediately from the market.¹³⁶ Since only Apple-manufac-

¹²⁶ See McCullagh, *supra* note 121.

¹²⁷ See *Sega Enters. v. Accolade, Inc.*, 977 F.2d 1510, 1527-28 (9th Cir. 1992) (stating “that where disassembly is the only way to gain access to the ideas and functional elements embodied in a copyrighted computer program and where there is a legitimate reason for seeking such access, disassembly is a fair use of the copyrighted work, as a matter of law”).

¹²⁸ *Lexmark Int’l, Inc. v. Static Control Components, Inc.*, 253 F. Supp. 2d 943, 974 (E.D. Ky. 2003).

¹²⁹ *Lexmark Int’l, Inc. v. Static Control Components, Inc.*, 2004 U.S. App. LEXIS 22250 (6th Cir. 2004).

¹³⁰ See Declan McCullagh, *Apple: Burn DVDs—and We’ll Burn You*, CNET NEWS (Aug. 28, 2002), at <http://news.com.com/2100-1023-955805.html>.

¹³¹ *Id.*

¹³² *Id.*

¹³³ *Id.*

¹³⁴ McCullagh, *supra* note 130.

¹³⁵ *Id.*

¹³⁶ See *id.*

tured internal drives can utilize iDVD, this will force consumers to purchase more computers since Apple does not offer this product as an upgrade.

As content providers have developed technological methods to restrict access to content legally acquired from different parts of the world,¹³⁷ the DMCA has been invoked to support these measures and thereby prohibit consumers from legitimately using this content. Sony has sued a number of manufacturers of so-called “mod chips” for alleged circumvention under the DMCA.¹³⁸ By invoking this strategy, Sony has been able to enforce a system of geographical regional restrictions raising significant anticompetitive issues.

“Mod chips” are after-market accessories that modify Sony Playstation consoles to allow games legitimately purchased in one part of the world to be played on a Playstation console from another geographic region.¹³⁹ In the U.S., Sony sued Gamemasters, Inc., distributor of the Game Enhancer peripheral device, which allowed U.S. Playstation users to play games purchased in Japan and other countries.¹⁴⁰ The court granted Sony’s injunction under the DMCA’s anti-circumvention provisions, thereby effectively banning the use of a technology that would permit consumers to use non-infringing games that were legitimately purchased from other regions.¹⁴¹ While Sony has argued that mod chips can enable the use of unauthorized copies of Playstation games,¹⁴² mod chips are capable of substantial non-infringing uses.¹⁴³ Consequently, public policy should weigh the use of the DMCA to enforce Sony’s region coding system, which prohibits the use of games legally purchased in other countries against any potentially illegitimate uses for such mod chips.

Like the chilling effect that the DMCA has had over scientific research, similar impacts are felt in the commercial setting. To encourage innovation and the development of interoperable products, access to copyright protected works must be allowed for reverse engineering purposes.

¹³⁷ See *Sony Computer Entm’t Am.*, 87 F. Supp. 2d 976; *Corley*, 273 F.3d at 451-53 (noting that the policy judgments require some legitimate uses of computer programs to be restricted because illicit use, which is the most frequent type of use, would be substantially harmful).

¹³⁸ See *Sony Computer Entm’t Am.*, 87 F. Supp. 2d at 977; see also Tony Smith, *Judge Deems PS2 Mod Chips Illegal in UK*, THE REGISTER (July 21, 2004) (noting Sony’s many suits to curtail the use of mod chips), available at http://www.theregister.co.uk/2004/07/21/ps2_mod_chip_win.

¹³⁹ See *Sony Computer Entm’t Am.*, 87 F. Supp. 2d at 981; see also Mod-chip.com, at http://www.mod-chip.com/faq_new.htm#10 (last visited Aug. 31, 2004).

¹⁴⁰ See *Sony Computer Entm’t Am.*, 87 F. Supp. 2d at 981-83.

¹⁴¹ *Id.* at 987-88.

¹⁴² See *id.* at 982.

¹⁴³ See Mod-chip.com, at <http://www.mod-chip.com/en/faq.htm#a1> (last visited Nov. 13, 2004).

The current anti-circumvention provisions of the DMCA are too restrictive and consequently will decrease the amount of innovation. If such policies continue unfettered, a monopolistic polarization of technology will evolve, creating a digital divide between copyright haves and have-nots.

IV. UNRESOLVED ISSUES AND POTENTIAL SOLUTIONS

In the absence of meaningful industry standards and agreements for the protection of digital content, the courts have stepped in and allowed the DMCA to be used as a sword against alleged infringers. However, these actions have created a set of confusing rulings that make it extremely difficult for a technologist to predict how the courts will rule on the use or development of new technologies. For example, two recent file-sharing cases have produced opposite results, which have created uncertainty regarding the application of the DMCA. In *MGM Studios, Inc. v. Grokster, Ltd.*, the court analyzed Grokster's peer-to-peer (P2P) file sharing network, which allowed users to share copyrighted digital content over the Internet, similar to the original Napster service.¹⁴⁴ The court held that the decentralized nature of the network limited Grokster's liability for the action of its users and thus could not be found liable under Section 501 of the DMCA.¹⁴⁵ However, the court in *In re Aimster Copyright Litigation*¹⁴⁶ found that a similar P2P file sharing system did not fall under any of the safe harbor provisions¹⁴⁷ allowed in the DMCA.

The fundamental struggle with which the courts are grappling involves the rights of the copyright holders versus the "fair use" rights of content owners. The majority of the efforts to date have focused on digital music files, as illustrated by *Grokster*¹⁴⁸ and *Aimster*,¹⁴⁹ but the battle will quickly expand to include digital video content as broadband connections become more ubiquitous. The courts ventured into the digital video realm in *Corley*,¹⁵⁰ but that case was more about the posting and linking of code to bypass the DVD encryption key as opposed to the usage rights of content owners.¹⁵¹ A major area of concern for copyright holders is the emergence of digital video recorders (DVR), devices that

¹⁴⁴ 259 F. Supp. 2d 1029, 1031-33 (C.D. Cal. 2003) *aff'd* 2004 U.S. App. LEXIS 17471 (9th Cir. 2004).

¹⁴⁵ *Id.* at 1041-43.

¹⁴⁶ *In re Aimster Copyright Litig.*, 334 F.3d 643 (7th Cir. 2003), *cert. denied*, 124 S.Ct. 1069 (2004).

¹⁴⁷ 17 U.S.C. § 512(i)(1)(A) (2000).

¹⁴⁸ *Grokster*, 259 F. Supp. 2d at 1031.

¹⁴⁹ *Aimster*, 334 F.3d at 645.

¹⁵⁰ *Corley*, 273 F.3d at 434.

¹⁵¹ *See id.* at 453-58.

allow a user to record content from television programs like a video cassette recorder (VCR) but store the information in digital format.

One particular device that is disconcerting to television networks and video copyright holders is the ReplayTV 4000, the first networked DVR with broadband connectivity that lets a user record up to 320 hours of television, playback recorded shows without commercials, and even share programs with other ReplayTV owners.¹⁵² Television networks are concerned about the ability of the ReplayTV 4000 to edit out commercials and then share this content with other users over the Internet.¹⁵³ The networks are also fearful that once programming material is captured in a digital format, it could easily be extracted and shared over the Internet via a peer-to-peer network.¹⁵⁴ Since digital copies are perfect copies of the original, the networks fear that users might abandon watching television in the regular method, preferring to watch commercial-less versions upon their convenience, which in turn would decrease the demand for commercial spots from advertisers and subscription fees derived from premium services.¹⁵⁵

In 2001, the three major television networks filed suit against the manufacturer of the ReplayTV 4000, claiming that the device would violate their copyrights by allowing users to share copies of programs over the Internet.¹⁵⁶ The networks stated that the device “deprives the copyright owners of the means by which they are paid for their creative content and thus reduces the incentive to create programming and make it available to the public.”¹⁵⁷ At the time the suit was filed, the ReplayTV device had not been released for sale to the public, but the networks sought an injunction to prevent the DVR from coming to market.¹⁵⁸ Ironically, the ReplayTV device does support a digital rights management system, thus giving networks the option to prevent users from sharing recorded programs.¹⁵⁹

The ReplayTV case is extremely important because it will help define the limits of consumer “fair use” for DVR devices. In 1984, the Supreme Court was faced with a similar challenge in *Sony Corporation*

¹⁵² ReplayTV website, at <http://www.digitalnetworksna.com/dvr/5500/features.asp> (last visited Aug. 31, 2004).

¹⁵³ Susan Rush, *Judge Allows Consumer Voice in DVR Court Fight*, CED BROADBAND DIRECT (Aug. 19, 2002), at http://www.broadbandweek.com/news/020819/020819_content_dvr.htm.

¹⁵⁴ See *id.*; see also *Corley*, 273 F.3d at 436.

¹⁵⁵ Rush, *supra* note 153.

¹⁵⁶ Associated Press, *Networks Sue Digital Recorder Maker*, N.Y. TIMES, Oct. 31, 2001, available at <http://2.mrbrklyn.com/resources/AP-Networks-ReplayTV.html>.

¹⁵⁷ *Id.*

¹⁵⁸ *Id.*

¹⁵⁹ *Id.*

of America v. Universal City Studios.¹⁶⁰ In that landmark case, the Court was asked to determine the limits of consumer fair use as applied to VCRs—new technology at the time that threatened the traditional views of copyright holders.¹⁶¹ At the time, the entertainment industry voiced some of the same arguments proposed by the opponents of ReplayTV, but did not realize the enormous potential associated with the sale and rental of videotapes which consumers could enjoy on their VCRs. In a surprising decision, the Court held that personal taping of television programs using a VCR device was “fair use,” and that the manufacturer of such devices were not contributory infringers.¹⁶²

The suit against the manufacturer of ReplayTV was eventually dropped for unspecified reasons,¹⁶³ but lingering questions still remain. In fact, a group of ReplayTV owners have recently joined together to seek a declaration regarding whether their use of the ReplayTV send-show and commercial-skipping features constitutes fair use or is copyright infringement.¹⁶⁴ It is likely that the DMCA will be addressed during this dispute, and prior court decisions will be heavily relied upon for their precedential value. There are two main issues to address, namely whether the use of the DVR device to skip commercials is permissible and whether the sharing of recorded programs with other DVR users infringes upon the rights of the copyright owner. In *Sony*,¹⁶⁵ the Court touched upon the use of a VCR to fast forward through commercials but did not issue a direct opinion on the matter, and instead held that personal “time-shifting” of commercial network television programs was permissible under fair use.¹⁶⁶ It is likely that a court will view the use of the ReplayTV’s commercial skipping feature in the same manner.

Based on cases like *Grokster*¹⁶⁷ and *Aimster*,¹⁶⁸ it is not clear how a court might rule regarding the file sharing capabilities of the ReplayTV. In *Grokster*, the decentralized design of the file-sharing architecture was determinative: the court decided that the P2P host could not be found liable for infringement because it lacked knowledge of any specific infringing activities.¹⁶⁹ Unlike some infamous digital music file-swapping networks where thousands of files can be easily shared among many anonymous users, the ReplayTV device actually limits file-sharing so

¹⁶⁰ 464 U.S. at 417.

¹⁶¹ *Id.* at 421-25.

¹⁶² *Id.* at 454-56.

¹⁶³ Michael Singer, *Networks Drop Lawsuit Against SONICblue*, CLICKZ NEWS (Nov. 27, 2001), at http://www.clickz.com/news/article.php/3531_929601.

¹⁶⁴ See *Newmark v. Turner Broad. Network*, 226 F. Supp. 2d 1215, 1218 (C.D. Ca. 2002).

¹⁶⁵ *Sony Corp.*, 464 U.S. at 448-50.

¹⁶⁶ *Id.* at 454-56.

¹⁶⁷ *Grokster*, 259 F. Supp. 2d 1029.

¹⁶⁸ *Aimster*, 334 F.3d 643.

¹⁶⁹ *Grokster*, 259 F. Supp. 2d at 1036-38, 1045-46.

that a recorded television broadcast cannot be sent to more than fifteen users.¹⁷⁰ Also, ReplayTV users can only share files with people they know, not with thousands of anonymous users.¹⁷¹

In the end, the question is whether the ReplayTV 4000 is more like the Sony Betamax VCR, which the Supreme Court ruled did not infringe copyright because the device was capable of “substantial non-infringing uses,”¹⁷² or more like Napster, one of the earliest file-sharing networks that was found to infringe copyright because it possessed knowledge of its users’ infringing activities.¹⁷³ For a court to rule that the ReplayTV 4000 infringes copyright, a potential plaintiff must demonstrate that any non-infringing uses of the device are insignificant.¹⁷⁴ However, this burden of proof could be very difficult to meet since the DVR device is capable of non-infringing uses similar to those associated with a VCR. It is likely that a court will find that the ReplayTV device does not infringe copyright based on much of the reasoning in *Sony*, provided that the file-sharing capabilities continue to be constrained to a small group.¹⁷⁵

As new technologies emerge, the DMCA will continue to be applied in ways that restrict many areas of copyright that have enjoyed protection under the Copyright Act.¹⁷⁶ However, the DMCA is an overly broad piece of legislation that prevents many of those privileges and needs to be re-evaluated to balance the interests of both copyright owners and consumers. Since the enactment of the DMCA, there have been numerous cases yielding unpredictable results and consequently producing a chilling effect on fair use, free speech, and innovation due to this uncertainty. Some modification to the DMCA is necessary to mitigate these chilling effects and allow the Copyright Act to fulfill its intended purpose—namely, to promote the progress of science and useful arts.¹⁷⁷

Some members of Congress are beginning to realize that the DMCA does not promote the beneficial effects of copyright protection and have recently introduced legislation to modify the DMCA. The most promising bill is the Digital Media Consumers Rights Act,¹⁷⁸ introduced by Representatives Boucher and Doolittle. One of the key features of this bill is the limitation placed on the scope of circumvention liability, restricting this liability to acts that have the sole purpose of infringing

¹⁷⁰ Doug Isenberg, *ReplayTV Lawsuit: Napster Redux?*, CNET News (Nov. 12, 2001), at <http://news.com.com/2010-1071-281601.html?legacy=cnet>.

¹⁷¹ *Id.*

¹⁷² *Sony Corp.*, 464 U.S. 417.

¹⁷³ *See A&M Records v. Napster, Inc.*, 239 F.3d 1004 (9th Cir. 2001).

¹⁷⁴ *See Sony Corp.*, 464 U.S. at 456.

¹⁷⁵ *See id.*

¹⁷⁶ 17 U.S.C. § 101 (2000).

¹⁷⁷ *See id.*

¹⁷⁸ *Digital Media Consumers’ Rights Act Section-by-Section Description*, available at <http://www.house.gov/boucher/docs/dmcrasec.htm>.

copyrights.¹⁷⁹ This will help minimize the fair use problem that is pervasive throughout the DMCA.

As discussed in Part Three, courts have applied the DMCA to suppress scientific research, resulting in a more restrictive marketplace of ideas. Restrictions on freedom in the academic setting will ultimately lead to less innovation; society as a whole will be worse off if the exchange of ideas continues to be hindered. Any modifications to the DMCA must carefully balance the needs of copyright holders and society to guard against any unintentional harm. Although the Digital Media Consumers Rights Act¹⁸⁰ acknowledges that the DMCA must be restructured, there are other legislative solutions to consider.

The DMCA gives force of law to any DRM system utilized by a copyright holder and consequently destroys the balance of bargaining rights between the copyright holder and consumers.¹⁸¹ Consequently, the rights of consumers, such as fair use and the right to make personal copies, are circumvented by technology that the DMCA makes illegal to bypass. However, the anti-circumvention clause of the DMCA has proven to be an ineffective measure for thwarting digital content piracy on the Internet.¹⁸² Although it might harm DRM and encryption technology producers, the anti-circumvention clause should be removed in favor of a return to traditional copyright principles.

The current version of the DMCA creates a perverse effect that encourages copyright holders to pursue litigation against individuals exercising their fair use rights, performing reverse engineering research, or even participating in legitimate, industry-sponsored challenges to crack a DRM system. These cases represent an offensive use of copyright law, as opposed to the traditional protective approach where a copyright holder is granted a fixed-length monopoly, after which time the work enters the public domain. Even if complete removal of the anti-circumvention clause does not generate enough support, modifying the language to allow for less-restrictive fair use applications may be prudent. For example, the clarification of non-infringing behavior in the security and encryption industries would result in positive benefits as academic researchers gain greater clarity over permissible activities. Digital security systems can only be strengthened by the free exchange of information and vigorous testing.

¹⁷⁹ *See id.*

¹⁸⁰ *Id.*

¹⁸¹ 17 U.S.C. § 1201(a) (2000).

¹⁸² In the four years following the introduction of the DMCA, CD sales per capita in United States have dropped thirty percent, suggesting that the DMCA has been ineffective in curbing digital piracy as p2p networks have grown in popularity. *See* Stan Liebowitz, *Pitfalls in Measuring the Impact of File-Sharing* (July 2004), available at <http://ssrn.com/abstract=583484>.

As a last alternative, Congress could elect to leave the DMCA untouched and allow the issues to be worked out in the courts. However, such an approach is not preferred over a legislative amendment because technology evolves at an extremely rapid pace while judicial solutions are historically inexpedient. As shown in this note, the DMCA has a chilling effect on various activities and will ultimately reduce the supply of borderline issues that could expand the body of law. This may lead to a stratification of current case law and see the chilling effect create a frozen tundra of uncertainty and stagnation.

CONCLUSION

Collisions between copyright law and new technologies are part of our copyright tradition; consider the player piano, broadcast radio, cable TV, and the VCR. In most cases, the copyright industries have evolved and prospered in the marketplace. On the few occasions where copyright industries have failed to adjust, Congress has stepped in with compulsory licensing. What Congress has not done is to regulate innovation in the name of copyright. Policy makers should be cautious when called upon to depart from our copyright traditions.

Copyright protection can only serve its intended purpose when the balance between owners and consumers is maintained. The Digital Millennium Copyright Act destroys that balance by granting too much power to the copyright owner. The Act is riddled with constitutional flaws and has rendered large parts of the traditional body of copyright law obsolete. The Act is being used as a sword to further extend the monopoly rights of copyright holders—a result contrary to the purpose of copyright protection. If this balance is not restored, society may find itself on slippery slope toward a state of affairs where copyrights become perpetual and freeze all future innovation. Society will be irreparably harmed if the shield that previously protected the expressive rights of society is allowed to become a sword to exert monopolistic rights on others.

