

THE DIGITAL MILLENNIUM COPYRIGHT ACT (DMCA) —
CONGRESS RESPONDS TO THE PERCEIVED IMBALANCE
BETWEEN CONTENT PROVIDERS AND USERS OF
COPYRIGHTED WORKS CAUSED BY ADVANCES IN
DIGITAL DISTRIBUTION TECHNOLOGIES
INCLUDING THE INTERNET

By:

Proprietary Rights Committee
Computer Law Section
State Bar of Michigan

Chairman

David R. Syrowik
Brooks & Kushman P.C.
Southfield, Michigan

Committee Members

Jonathan R. Alger
Roland J. Cole
Sandra Jo Franklin
Mitchell A. Goodkin
William M. Hanlon, Jr.
Mary I. Hiniker
John S. LeRoy
Ronald M. Nabozny
Paul J. Raine

*State Bar of Michigan
66th Annual Meeting
September 12, 2001
Lansing, Michigan*

TABLE OF CONTENTS

	<u>Page</u>
I. INTRODUCTION	1
II. THE INTERNET	5
III. THE COPYRIGHT SYSTEM	7
IV. THE DIGITAL MILLENNIUM COPYRIGHT ACT (DMCA)	10
A. Background And Structure Of The DMCA	10
B. Section 1201's Anti-Circumvention Bans	11
C. Statutory Exemptions To The Bans	13
D. Case Law.....	17
V. CONCLUSION.....	20

Appendix A - The Digital Millennium Copyright Act

Appendix B - Description of Phases 1 and 2 of the SDMI

I. INTRODUCTION

Many companies, both new and old, depend at least in part on the Internet. For example, Napster implemented a system that indexed music files on individuals' computer hard drive and that facilitated computer-to-computer transfer of these files over the Internet.¹

In a highly publicized lawsuit by the record companies against Napster,² Napster has recently been found to be an infringer under the Copyright Act of 1976. The court applied the traditional doctrines of contributory³ and vicarious copyright infringement⁴ but not without some controversy associated therewith.⁵

¹ The files store audio recordings in a digital format called MPEG-3 (MP3). Through a process called "ripping," a computer user can copy an audio CD directly onto a computer hard drive in MP3 format. Napster does not participate in the actual ripping, nor does it actually store ripped files on its system. However, Napster does facilitate access to and transmission of ripped files that are stored on individual hard drives.

² The district court preliminarily enjoined Napster "from engaging in, or facilitating others in copying, downloading, uploading, transmitting or distributing plaintiffs' copyrighted musical compositions and sound recordings . . . without express permission of the rights owner." *A&M Records, Inc. v. Napster, Inc.*, 114 F.Supp.2d 896, 927 (N.D. Cal. 2000). The Ninth Circuit temporarily stayed the preliminary injunction pending appeal. After considering the parties' arguments, the Ninth Circuit affirmed the District Court's decision that Napster was liable as a contributory and vicarious infringer, but again stayed the preliminary injunction pending the district court's modification, on remand, of the overbroad injunction, consistent with the Ninth Circuit's opinion. *A&M Records, Inc. v. Napster, Inc.*, 239 F.3d 1004 (9th Cir. 2001).

³ Unlike the patent statute, the copyright statute does not have express language regarding contributory infringement. However, "[T]he absence of . . . express language in the copyright statute does not preclude the imposition of liability for copyright infringements on certain parties who have not themselves engaged in the infringing activity for vicarious liability is imposed in virtually all areas of the law, and the concept of contributory infringement is merely a species of the broader problem of identifying the circumstances in which it is just to hold one individual accountable for the actions of another." *Sony Corp. v. Universal City Studios, Inc.*, 464 U.S. 417, 435 (1984). "[O]ne who, with knowledge of the infringing activity, induces, causes or materially contributes to the infringing conduct of another, may be held liable as a contributory infringer." *Sega Enters. Ltd. v. MAPHIA*, 857 F.Supp. 679, 686 (N.D. Cal. 1994).

⁴ "A defendant is liable for vicarious liability for the actions of a primary infringer where the defendant (1) has the right and ability to control the infringer's acts and (2) receives a direct

In late 1998, the U.S. Congress enacted the Digital Millennium Copyright Act (DMCA),⁶ the most sweeping revisions ever to the Copyright Act of 1976. The DMCA was enacted in large part in response to the unique threat to the rights of copyright owners caused by the technological advancements which came quickly during the 1990s which made mass copying and transmission of copyrighted works over the Internet practical.⁷

The DMCA not only prohibits circumvention of technological measures that control access to copyrighted works (such as copy-protection systems and encryption technologies)⁸, but also prohibits trafficking in any technology desired to accomplish such circumvention⁹ or any technology designed to “protect a right” of a copyright owner under the

financial benefit from the infringement. . . . Unlike contributory infringement, knowledge is not an element of vicarious liability.” *Religious Technology Ctr. v. Netcom On-line Com. Servs., Inc.*, 907 F.Supp. 1361, 1375 (N.D. Cal. 1995) (citations omitted).

⁵ Part of the controversy arises because Napster provides music listeners choice, convenience and flexibility that they’ve never before experienced. From a legal perspective, Napster can be used, and to some extent is used, for the distribution of public domain files and for the distribution of files with permission of the copyright owner. Under *Sony*, Napster need only show that it was “capable of substantial noninfringing uses.” “[T]he sale of copying equipment, like the sale of other articles of commerce, does not constitute contributory infringement if the product is widely used for legitimate, unobjectionable purposes. Indeed, it need merely be capable of substantial noninfringing uses.” *Sony Corp. v. Universal City Studios, Inc.*, 464 U.S. 417, 442 (1984).

⁶ See Appendix A to this report for a copy of new Chapter 12 the Copyright Act.

⁷ Advancements such as MP3 compression, cable modems, DSL, inexpensive storage media have enabled users of the Internet to create millions of perfect copies of musical works and distribute these copies to millions of computer users within a very short period of time.

⁸ “[T]o descramble a scrambled work, to decrypt an encrypted work, or otherwise to avoid, bypass, remove, deactivate, or impair a technological measure, without the authority of the copyright owner.” 17 U.S.C. § 1201(a)(3)(A).

⁹ 17 U.S.C. § 1201(a)(2).

Copyright Act.¹⁰ The “anti-circumvention” bans of the DMCA represent a change in Congress’ efforts to balance the interests of copyright owners and the interests of the users of copyrighted works.¹¹ A recent case¹² has provided an initial interpretation of the DMCA and, in view of that interpretation, the DMCA appears to involve a dramatic shift in rights from users of copyrighted works to content providers.

After providing a brief overview of the Internet and the Copyright System prior to the DMCA, this report discusses the DMCA in some detail and the few cases that have interpreted it to determine how radical or dramatic this shift of rights from users to providers may be. In particular, how much more difficult has the DMCA made it for content users to take advantage of some of the long important exceptions to copyright protection such as “first sale,” “fair use,” and the First Amendment?

¹⁰ 17 U.S.C. § 1201(b).

¹¹ “Historically, Congress has achieved the objectives of the Constitution’s Copyright Clause ‘by regulating the use of information--not the devices or means by which the information is delivered or used by information consumers--and by ensuring an appropriate balance between the interests of copyright owners and information users.’ The various provisions of the Copyright Act, on the one hand creating rights for proprietors but on the other hand delineating the scope of those rights, have as a unifying theme the fact that they are all ‘technology neutral.’ That is to say, those laws do not regulate commerce in information technology, i.e., products and devices for transmitting, storing, and using information. Instead, they prohibit certain actions and create exceptions to permit certain conduct deemed to be in the greater public interest, all in a way that balances the interests of copyright owners and users of copyrighted works.” Nimmer, A RIFF ON FAIR USE IN THE DIGITAL MILLENNIUM COPYRIGHT ACT, 148 U. Pa. L. Rev. 673, 683 (2000) (footnotes omitted).

¹² *Universal City Studios, Inc. v. Reimerdes*, 111 F.Supp.2d 294 (S.D.N.Y. 2000).

II. THE INTERNET

The following facts about the Internet were found by the district court in the case *ACLU v. Reno*,¹³ which invalidated the Communications Decency Act, Congress' first attempt to regulate the Internet. These facts are very instructive as to the capabilities and power of the Internet.

The Internet is not a physical or tangible entity, but rather a giant network which interconnects innumerable smaller groups of linked computer networks. It is thus a network of networks. . . . Many networks . . . are connected to other networks, which are in turn connected to other networks in a manner which permits each computer in any network to communicate with computers on any other network in the system. This global Web of linked networks and computers is referred to as the Internet.¹⁴

No single entity — academic, corporate, governmental, or non-profit — administers the Internet. It exists and functions as a result of the fact that hundreds of thousands of separate operators of computers and computer networks independently decided to use common data transfer protocols to exchange communications and information with other computers (which in turn exchange communications and information with still other computers). There is no centralized storage location, control point, or communications channel for the Internet, and it would not be technically feasible for a single entity to control all of the information conveyed on the Internet.¹⁵

Once one has access to the Internet, there [is] a wide variety of different methods of communication and information exchange over the network. These many methods of communication and information retrieval are constantly evolving and are therefore difficult to categorize concisely. The most common methods of communications on the Internet (as well as within the major online services) can be roughly grouped into six categories:

¹³ *American Civil Liberties Union v. Reno*, 929 F.Supp. 824 (E.D. Pa. 1996), *aff'd*, *Reno v. American Civil Liberties Union*, 521 U.S. 844 (1997).

¹⁴ *Ibid*, pp. 830-31.

¹⁵ *Ibid*, pp. 831-32.

- (1) one-to-one messaging (such as “e-mail”),
- (2) one-to-many messaging (such as “listserv”),
- (3) distributed message databases (such as “USENET newsgroups”),
- (4) real time communication (such as “Internet Relay Chat”),
- (5) real time remote computer utilization (such as “telnet”),
and
- (6) remote information retrieval (such as “ftp,” “gopher,” and the “World Wide Web”).

Most of these methods of communication can be used to transmit text, data, computer programs, sound, visual images (i.e., pictures), and moving video images.¹⁶

The following quotes from other case law also help to explain the capabilities of the technology of the Internet:

The Internet is more than a means of communications; it also serves as a conduit for transporting digitized goods, including software, data, music, graphics, and videos which can be downloaded from the provider’s site to the Internet user’s computer.¹⁷

Until recently, the Internet was of little use for the distribution of music because the average music computer file was simply too big: the digital information on a single compact disc of music required hundreds of computer floppy discs to store, and downloading even a single song from the Internet took hours. However, various compression algorithms (which make an audio file “smaller” by limiting the audio bandwidth) now allow digital audio files to be transferred more quickly and stored more efficiently.¹⁸

¹⁶ *Ibid.*, p. 834.

¹⁷ *American Library Association v. Pataki*, 969 F.Supp. 160, 173 (S.D.N.Y. 1997).

¹⁸ *Recording Indus. Ass’n of America v. Diamond Multimedia Sys., Inc.*, 180 F.3d 1072, 1073-74 (9th Cir. 1999).

III. THE COPYRIGHT SYSTEM

After a period of gestation over some twenty years, Congress exercised its constitutional power of “securing for limited times” to “authors” the “exclusive right” to their “writings”¹⁹ in the Copyright Act of 1976, now codified in Title 17 of the U.S. Code. Section 102(a) of the Act states that copyright protection is available for “original works of authorship,” whereas Section 102(b) of the Act states that copyright protection does not extend to “any ideas, procedure, process, system, method of operation, concept, principle or discovery.”²⁰

The Supreme Court has stated that:

The primary objective of copyright is not to reward the labor of authors, but “[t]o promote the Progress of Science and useful Arts.” . . . To this end, copyright assures authors the right to their original expression, but encourages others to build freely upon the ideas and information conveyed by a work. This principle, known as the idea/expression or fact/expression dichotomy, applies to all works of authorship. . . . This result is neither unfair nor unfortunate. It is the means by which copyright advances the progress of science and art.”²¹

The scheme of the Copyright Act is to provide a broad grant of certain rights to copyright owners in Section 106 of the Act and then to place limitations upon these rights in Section 107f.f.

¹⁹ U.S. Const., Art. 1, Sec. 8, cl. 8.

²⁰ Section 102(b) thereby codifies the long-held principle of *Baker v. Seldon*, 101 U.S. 99 (1880), that copyright on a book does not give the author exclusive rights to any methods of operation described in the book.

²¹ *Feist Publications, Inc. v. Rural Tel. Serv. Co.*, 499 U.S. 340, 349 (1991) (citations omitted) (Copyright protection does not extend to facts and data *per se* but rather only to original selections, coordinations and arrangements of such facts and data under Section 103(b) of the Act).

For example, Section 106 affords a copyright owner the exclusive right to:

(1) reproduce the copyrighted work; (2) prepare derivative works; (3) distribute copies of the work by sale or otherwise; and, with respect to certain artistic works, (4) perform the work publicly; and (5) display the work publicly.

One of the most important limitations of Section 106 is the doctrine of “fair use.” Prior to the Copyright Act of 1976, “fair use” was merely a judicial doctrine wherein copying of protected works was permitted in certain various circumstances. “Fair use,” however, was codified in Section 107 of the Act.²² (4) the effect of the use upon the potential market for or the value of the copyrighted work.”

One court has characterized Section 107 as “a codification of the decisional law in an effort to prevent rigid application of the Copyright Act where such application would unreasonably prevent the dissemination of information.”²³

However, another court has gone further by stating that “since the passage of the 1976 Act, “fair use” should no longer be considered an infringement to be excused; instead, it is logical to view “fair use” as a right.”²⁴

²² Section 107 states: “Notwithstanding the provisions of sections 106 and 106A, the fair use of a copyrighted work, including such use by reproduction in copies or phonocopies or by any other means specified in that section, for purposes such as criticism, comment, news reporting, teaching . . . scholarship, or research is not an infringement of copyright. In determining whether the use made of a work in any particular case is a fair use the factors to be considered shall include —

(1) the purpose and character of the use;
(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

²³ *Consumers Union of the United States, Inc. v. General Signal Corp.*, 724 F.2d 1044, 1096 (2d Cir. 1983).

²⁴ *Bateman v. Mnemonic, Inc.*, 79 F.3d 1532, 1542 n.22 (11th Cir. 1995).

Another important limitation of Section 106 of the Copyright Act is Section 109, sometimes referred to as the “first sale doctrine.” This doctrine prohibits the owner of a copyright in a work from limiting the sale or distribution of copies of that work that have been lawfully acquired.²⁵ Both the fair use doctrine and the first sale doctrine have accorded the public substantial leeway in browsing published works.

²⁵ It is important to note the distinction between owning a copy of the work and the copyright in the work. As noted in Section 202 of the Act: “Ownership of a copyright, or of any of the exclusive rights under a copyright, is distinct from ownership of any material object in which the work is embodied. Transfer of ownership of any material object, including the copy or phonorecord in which the work is first fixed, does not of itself convey any rights in the copyrighted work embodied in the object; nor, in the absence of an agreement, does transfer of ownership of a copyright or of any exclusive rights under a copyright convey property rights in any material object.”

IV. THE DIGITAL MILLENNIUM COPYRIGHT ACT (DMCA)

A. Background And Structure Of The DMCA

The *Reimerdes* case provides an excellent background and structure of the DMCA as follows:

In December 1996, the World Intellectual Property Organization (“WIPO”), held a diplomatic conference in Geneva that led to the adoption of two treaties. Article 11 of the relevant treaty, the WIPO Copyright Treaty, provides in relevant part that contracting states “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 restricts acts, in respect of their works, which are not authorized by the authors concerned or permitted by law.”

The adoption of the WIPO Copyright Treaty spurred continued Congressional attention to the adaptation of the law of copyright to the digital age. Lengthy hearings involving a broad range of interested parties both preceded and succeeded the Copyright Treaty. As noted above, a critical focus of Congressional consideration of the legislation was the conflict between those who opposed anti-circumvention measures as inappropriate extensions of copyright and impediments to fair use and those who supported them as essential to proper protection of copyrighted materials in the digital age. The DMCA was enacted in October 1998 as the culmination of this process.

The DMCA contains two principal anti-circumvention provisions. The first, Section 1201(a)(1), governs “[t]he act of circumventing a technological protection measure put in place by a copyright owner to control access to a copyrighted work,” an act described by Congress as “the electronic equivalent of breaking into a locked room in order to obtain a copy of a book.” The second, Section 1201(a)(2), which is the focus of this case, “supplements the prohibition against the act of circumvention in paragraph (a)(1) with prohibitions on creating and making available certain technologies . . . developed or advertised to defeat technological protections against unauthorized access to a work.”²⁶

²⁶ *Supra*, note 12 at pp. 315-16.

Section 103 of the DMCA adds sections 1201-1205 to the Copyright Act, implementing the WIPO Treaties provisions prohibiting the circumvention of technological copyright protection measures and protecting the integrity of “copyright management information.” Sections 1201 and 1202 define such prohibited conduct, while Sections 1203 and 1204 establish civil remedies and criminal penalties for violation of Sections 1201 and 1202. Section 1205 essentially provides that a violation of Sections 1201 and 1202 does not mitigate or provide a defense to the violation of an Internet user’s privacy caused by a technological copyright protection measure.

B. Section 1201’s Anti-Circumvention Bans

Section 1201(a)(1)(A) of the DMCA provides protection to encourage copyright owners to make their works available over the Internet and in other digital formats, by prohibiting individuals from “circumventing a technological measure.” What this means is that the DMCA punishes people for attempting to disable or bypass a technological measure intended to guard a copyrighted work of authorship. Examples of the sort of technological measures envisioned by the statute are passwords and encryption codes. Thus, if a software developer has encrypted his software to protect it from piracy, the DMCA sanctions anyone who attempts to impair or incapacitate the encryption device. The act of circumventing a technological protection measure put in place by a copyright owner to control access to a copyrighted work is the electronic equivalent of breaking into a locked room in order to obtain a copy of a book as noted above. This provision can be called the “basic provision” of the Section 1201 anti-circumvention bans which took effect on October 22, 2000.

Section 1201(a)(2) of the Act prohibits the manufacture or sale of devices primarily designed to circumvent control access technology. The trafficking ban does not target those who break into the locked room, but instead those who facilitate the process — say, those who market burglar’s tools. This provision can be called the “trafficking” ban, and took effect on October 28, 1998.

Section 1201(b)(1) of the Act prohibits the manufacture or sale of a device designed to circumvent a technology which protects any of the copyright rights of a copyright owner. In other words, while this provision does not prevent access to a copyrighted work, it prevents the trafficking of devices which disable technologies, which protect the work from, for example, being copied or distributed such as “watermarking” technology.²⁷ This technology may be used to prevent widespread reproduction and distribution of digital material. Such technology is becoming available by the secure digital music initiative (SDMI) — a group of hardware and software companies and recording industry representatives who have joined forces to develop a new compression format that would enable music providers to control in various ways the ability of users to copy or alter the encoded material. The members of SDMI have decided to move forward on two tracks: Phase 1 and Phase 2, as described in greater detail in Appendix B. This provision can be called the “additional violations” ban.

C. Statutory Exemptions To The Bans

²⁷ A digital watermark is “[A] small, almost unnoticeable alteration to a digital work like an image, a photograph, or a sequence of sounds. The watermark cannot be perceived with the human eye, but can be detected with a computer program designed for the purpose. Watermarks can be used to embed identifying information into the digital work.” I. Trotter Hardy, *Project Looking Forward: Sketching the Future of Copyright in a Networked World* 14 (May 1998).

The vast bulk of Section 1201 comprises its numerous exemptions, some of which apply to the “basic provision” alone, others to the “basic provision” along with the “trafficking ban” and others still to all three bans.

The exemption of Section 1201(d) in favor of nonprofit libraries, archives, and educational institutions applies only to the basic provision. It furnishes no defense to the trafficking ban and additional violations. Such conduct must be for the sole purpose of making a good faith determination of whether to acquire a work. The upshot is that a library can obtain unauthorized access to a copyrighted work through this vehicle, but cannot manufacture or distribute devices or systems that either facilitate that access, or that take works to which access has been granted and defeat use restrictions put in place by the copyright owner.

The Section 1201(i) exemption appears to be directly aimed at the use of “cookies” by many Web sites.²⁸ Although “cookies” are a useful marketing tool for Web site operators, they are generally viewed by Internet users as intrusive and unwelcome. In response, Internet users often configure their Web browsers to reject attempts to create “cookies” on their computers or employ readily available programs designed to delete such files. The user privacy provision of § 1201(i) allowing for the deactivation of “cookies” likewise attaches only to the basic provision, rather than to the other two bans.

²⁸“Cookie” technology allows a Web site’s server to place information about a consumer’s visits to the site on the consumer’s computer in a text file that only the Web site’s server can read. Using cookies a Web site assigns each consumer a unique identifier (not the actual identity of the consumer), so that the consumer may be recognized in subsequent visits to the site. On each return visit, the site can call up user-specific information, which could include the consumer’s preferences or interests, as indicated by documents the consumer accessed in prior visits or items the consumer clicked on while in the site.” Federal Trade Commission, *Privacy Online: A Report to Congress* n.4 (June 1998).

The exemption under Section 1201(e) is not limited to traditional law enforcement and intelligence agencies, but applies to any agency engaged in a lawfully authorized law enforcement or intelligence activity. The exemption of Section 1201(e) acts as an exception to Section 1201 as a whole. It therefore serves as a limitation on each of the three bans.

Section 1201(f) creates a narrowly limited “reverse engineering” exemption for the circumvention of technological measures controlling access to a computer program. The Section 1201(f) exemption applies to the reverse engineering of copyrighted computer programs for the sole purpose of identifying and analyzing those elements of the protected work “necessary to achieve interoperability” with other independently created programs.²⁹

“Allowing a computer programmer to hide his ideas, processes and concepts in copyrighted object code defeats the fundamental purpose of the Copyright Act to encourage the creation of original works by protecting the creator’s expression while leaving the ideas, facts, and functional concepts in the free marketplace to be built upon by others.” *DSC Comm. Corp. v. DGI Technologies, Inc.*, 898 F.Supp. 1183, 1191 (N.D. Tex. 1995), *aff’d*, 81 F.3d 597 (5th Cir. 1996). For purposes of Section 1201(f), interoperability is defined as the ability of computer

²⁹ “Interoperability” is just one reason to allow reverse engineering. The case law in the computer software copyright law area is much more generous.

“An author cannot acquire patent-like protection by putting an idea, process, or method of operation in an unintelligible format and asserting copyright infringement against those who try to understand that idea, process, or method of operation.” *Atari Games Corp. v. Nintendo of America, Inc.*, 975 F.2d 832, 842 (Fed. Cir. 1992).

“When the nature of a work requires intermediate copying to understand the ideas and processes in a copyrighted work, that nature supports a fair use for intermediate copying. Thus, reverse engineering object code to discern the unprotectable ideas in a computer program is a fair use.” *Id.* at 843.

programs to exchange and share information. One portion of the reverse engineering exemption of Section 1201(f) applies to the basic provision. Separate portions apply to the other two bans.

Section 1201(g) creates an exemption for the circumvention of technological measures controlling access to a copyrighted work for the sole purpose of “encryption research.” The purpose of Section 1201(g) is to promote the development of encryption-based protective measures for copyrighted works and other sensitive materials. One portion of the encryption exemption of Section 1201(g) applies to the basic provision, and another to the ban on trafficking. There is, however, no exemption here from the “additional violations.”

Section 1201(j) creates an exemption for the circumvention of technological measures controlling access to a copyrighted work for the sole purpose of “security testing.” Security testing is defined as accessing a computer system or network for the sole purpose of “investigating, or correcting, a security flaw or vulnerability,” with the authorization of the owner of the computer system or network. Exemptions for security testing of Section 1201(j) apply to the basic provision and trafficking ban but not to the “additional violations.”

Based on the above bans and exemptions, the following observations can be made:

- 1) There is no general right to browse (*i.e.*, via “fair use” or “first sale”) access-protected works. The “fair use” defense noted in Section 1201(c)(1) is only a defense for copyright infringement, not for the bans of Section 1201. Only limited exemptions are provided such as for qualifying libraries and archives. Individuals generally do not have such rights.

2) The trafficking ban prevents individuals or companies from marketing technological solutions to others who may have an exception but are unable to internally develop such technological solutions. Consequently, the only users whose interests are truly safeguarded are those who possess sufficient expertise to whatever “technological measures” are placed in their paths.

The following table summarizes the various bans and the applicable exemptions.

Anti-Circumvention Bans

	<u>Basic Provision</u> cannot circumvent a measure that controls “access” to a copyrighted work (§ 1201(a)(1))	<u>Trafficking</u> cannot traffic is something that circumvents a technological measure that controls “access” (§ 1201(a)(2))	<u>Additional Violations</u> cannot traffic is something that circumvents a technological measure that protects a copyright right (§ 1201(b))	
Exemptions	Non-profit libraries, archives and educational institutions (§ 1201(d))	yes	no	no
	User privacy (i.e., deactivation of “cookies”) (§ 1201(i))	yes	no	no
	law enforcement or intelligence activities (§ 1201(e))	yes	yes	yes

	<u>Basic Provision</u> cannot circumvent a measure that controls “access” to a copyrighted work (§ 1201(a)(1))	<u>Trafficking</u> cannot traffic is something that circumvents a technological measure that controls “access” (§ 1201(a)(2))	<u>Additional Violations</u> cannot traffic is something that circumvents a technological measure that protects a copyright right (§ 1201(b))
reverse engineering (but only interoperability) (§ 1201(f))	yes	yes	yes
encryption research (§ 1201(g))	yes	yes	no
security testing (§ 1201(j))	yes	yes	no

D. Case Law

In August of 2000, Judge Louis Kaplan of the Southern District of New York preliminarily enjoined a computer hacker online magazine (2600.com) for violating Section 1201(a)(2), the anti-trafficking provision, by posting on the Internet decryption software (DeCSS) that permits the copying of movies on DVD disks. He also found that none of the reverse engineering exceptions to those provisions applied, and that the injunction did not violate the First Amendment by prohibiting the dissemination of computer software as speech.³⁰

³⁰ *Supra*, note 12.

Later in the decision in discussing the constitutionality of the DMCA with respect to the First Amendment, Judge Kaplan stated that:

. . . the anti-trafficking provision of the DMCA may prevent technologically unsophisticated persons who wish to copy portions of DVD movies for fair use from obtaining the means of doing so. It is the interests of these individuals upon which defendants rely most heavily in contending that the DMCA violates the First Amendment because it deprives such persons of an asserted constitutional right to make fair use of copyrighted materials.

In a footnote to this part of the opinion, the Court perhaps raised an even larger specter:

The same point might be made with respect to copying of works upon which copyright has expired. Once the statutory protection lapses, the works pass into the public domain. The encryption on a DVD copy of such a work, however, will persist. Moreover, the combination of such a work with a new preface or introduction might result in a claim to copyright in the entire combination. If the combination then were released on DVD and encrypted, the encryption would preclude access not only to the copyrighted new material, but to the public domain work. As the DMCA is not yet two years old, this does not yet appear to be a problem, although it may emerge as one in the future.

On appeal, the hacker magazine is challenging the legislation as an improper impediment to legitimate fair uses of copyrighted material and as a burden on the exercise of First Amendment rights.³¹

A preliminary injunction based on 17 § 1201(a)(2) was granted in the case *RealNetworks, Inc. v. Streambox, Inc.*³² *RealNetworks*, with permission of copyright owners, delivered “streaming” audio and video over the Internet. At the insistence of the copyright owners, *RealNetworks* used cryptographic techniques to ensure that Internet users could not

³¹ *Universal City Studios, Inc. v. Reimerdes*, 2d Cir., No. 00-9185, argued on 5/1/01.

³² 2000 U.S. Dist. Lexis 1889 (W.D. Wash. 2000).

record the audio and video streams. *Streambox* broke the codes and distributed software that allowed ordinary Internet users to record the audio and video transmitted by *RealNetworks*.

One of the offending *Streambox* products was the *Streambox* VCR. The VCR mimics a RealPlayer and circumvents a Secret Handshake and ignores Copy Switch control features of the *RealNetworks*' products, allowing users to gain unauthorized access to content being sent via RealServers. The Court found that the VCR product was designed to circumvent technological measures afforded to *RealNetworks*' customers and that it was marketed as such.

The Court stated:

The portions of the VCR that circumvent the secret handshake and copy switch permit customers to obtain and redistribute perfect digital copies of audio and video files that copyright owners have made clear they do not want copied. For this reason, *Streambox*'s VCR is not entitled to the same “fair use” protections the Supreme Court afforded to video cassette recorders used for “time-shifting” in *Sony Corp. v. Universal City Studios, Inc.*, 464 U.S. 417 (1984).

Consequently, the Court explicitly stated that the *Sony* doctrine will not insulate manufacturers from a circumvention claim.

V. CONCLUSION

Advances in digital network technologies, such as the Internet, for the distribution of copyrighted subject material caused Congress to pass the DMCA in order to make such networks safe places to disseminate and exploit copyrighted materials. Neither “fair use” nor the First Amendment appear to be defenses to a cause of action arising under the DMCA. Although well-meaning, the anti-trafficking provisions of the DMCA appear to unfairly penalize those

who do not personally possess sufficient expertise to counteract whatever technological measures are placed in their paths. Finally, while not yet a problem, it appears that content providers can take advantage of the DMCA to protect subject matter not eligible for copyright protection by appending copyrightable subject matter to it and then encrypting the resulting work.