Reconciling Software Technology and Anti-circumvention Provisions in the Digital Millenium Copyright Act

Myron Hecht*

J.D., UCLA, 2003

Myron Hecht is employed at the Aerospace Corporation, a Federally Funded Research and Development Center in El Segundo, California. He works on both legal and engineering issues in software, certification, and safety for major satellite programs. In addition to his law degree, Mr. Hecht holds an M.S. in Engineering and an M.B.A., both from UCLA. He has previously published on products liability issues associated firmware in consumer products as well as technical articles in systems reliability, software engineering, and fault tolerant computing

Abstract

Section 1201 of the U.S. Copyright Act (part of the Digital Millenium Copyright Act) prohibits the circumvention of copy and access protection on data streams, files, and storage media containing digital copyrighted material. Although they have been affirmed by the courts, these prohibitions are highly controversial because they effectively ban reverse engineering and inhibit public discussion on computer security issues in the software development community. The root cause of these criticisms is the mismatch between the legal-conceptual framework of the DMCA and the largely abstract, flexible, and amorphous nature of software. The mismatch has resulted in the following difficulties: (a) separating the functional and expressive aspects of software, (b) defining the limits of permissible reverse engineering for software that contains function, copy protection, and access control measures, (c) distinguishing access control from copy protection, and (d) determining whether the function or market value of suspect software is primarily for circumvention or for its functionality. This Article elaborates on these difficulties and proposes three solutions: (1) requiring that copyright holders explicitly isolate and label copy and access protection measures that would fall under the anti-circumvention measures, (2) exempting from circumvention firmware contained in utilitarian articles that were not previously allowed copyright protection, and (3) explicitly allowing free discussion of security, encryption, and circumvention of existing measures so long as such discussions do not include compilable or executable computer software.

I. Introduction

The Digital Millennium Copyright Act (DMCA)[1] is a complex piece of legislation written for many purposes, one of which was to encourage the distribution of copyrighted content over the Internet by explicitly prohibiting persons from defeating (circumvening) the copy and access control measures that copyright holders might use to prevent infringement. However, the DMCA anti-circumvention prohibitions are quite broad and have been criticized as an undue intrusion on areas of computer research and development that were previously unrestricted. As an increasing number of court decisions have affirmed anti-circumvention prohibitions within the act, such criticism has grown.[2]

Section 1201, of the portion of the DMCA covering anti-circumvention prohibitions, has been criticized as a threat to civil liberties, academic freedom, and the flow of knowledge.[3] The opposition to section 1201 has increased due to events such as a

---

[1] The Digital Millennium Copyright Act, Pub. L. No. 105-304, 112 Stat. 2860 (1998), is divided into five titles, the "WIPO Copyright and Performances and Phonograms Treaties Implementation Act of 1998"; the "Online Copyright Infringement Liability Limitation Act"; the "Computer Maintenance Competition Assurance Act"; miscellaneous provisions; and the "Vessel Hull Design Protection Act". This paper concentrates on portions of Title I. These provisions were enacted by Congress to be responsive to a World Intellectual Property Organization (WIPO) copyright treaty requirement to "provide adequate legal protection" and "effective legal remedies" against those who would circumvent "technical protections." H.R. Rep. No. 105-551, pt. 1, at 9-11, pt. 2, at 21-24 (1998) (discussing legislative history of the DMCA).

[2] *See, e.g.*, Electronic Frontier Foundation, "Unintended Consequences: Five Years under the DMCA" (Sept. 24, 2003), *at* http://www.eff.org/IP/DMCA/unintended_consequences.php (last visited Nov. 12, 2003). *See also* Lev Ginsburg, "Anti-Circumvention Rules and Fair Use" (2002), 2002 UCLA J.L. & Tech. 4 *at* http://www.lawtechjournal.com/articles/2002/04_021027_ginsburg.php (last visited Nov. 12, 2003); Ronald S. Katz and Adam J. Safer, "Whither the DMCA? A Tale of Two Cases", Computer Law Association, *at* http://www.cla.org/a_tale_of_two_cases_dmca.htm (last visited Oct. 30, 2003).

[3] *See, e.g.*, Letter signed by Edward W. Felten, Princeton University; Edward D. Lazowska, University of Washington, Co-chair, Computing Research Association, Government Affairs Committee; Barbara Simons, Co-chair, Association of Computing Machinery US Public Policy Committee (Aug. 19, 2002), *available at* http://www.politechbot.com/p-03912.html (last visited Nov. 1, 2003). *See also* Electronic

the criminal prosecution of a Russian programmer and his employer,[4] the widely publicized withdrawal of a paper from a technical conference by a professor in the Department of Computer Science at Princeton University,[5] injunctions requiring the removal of links to DVD copying software,[6] the criminal prosecution of a young Norwegian programmer for developing software to circumvent the industry standard DVD copying protection system,[7] the producer of off-brand laser printer toner cartridge replacements for a major printer brand,[8] and the developer of a replacement garage door opener.[9]

The root cause of these criticisms is a mismatch between the legal-conceptual framework of the DMCA and the largely abstract, flexible, and amorphous nature of software. The mismatch has resulted in the following fact finding and legal interpretation difficulties: (a) separating the functional and expressive aspects of software, (b) defining the limits of permissible reverse engineering for software that contains function, copy protection, and access control measures, (c) distinguishing access control from copy

---

Frontier Foundation, "Unintended Consequences: Five Years under the DMCA" (Sept. 24, 2003), *at* http://www.eff.org/IP/DMCA/unintended-consequences.php (last visited Nov. 12, 2003).

[4] United States v Elcom Ltd., 203 F. Supp. 2d 1111 (N.D. Cal. 2002).

[5] Princeton Univ. Department of Computer Science, Secure Internet Programming, "Status of the paper 'Reading Between the Lines: Lessons from the SDMI Challenge'" Aug. 15, 2001), *at* http://www.cs.princeton.edu/sip/sdmi/ (last visited May 9, 2003).

[6] Universal City Studios, Inc. v. Corley, 2000 U.S. Dist. LEXIS 10621 (S.D.N.Y. 2000).

[7] "Norwegian Teenager Jon Johansen Acquitted in DVD Case", *ITsecurity.com*, *at* http://www.itsecurity.com/tecsnews/jan2003/jan42.htm (last visited May 9, 2003).

[8] Lexmark Int'l, Inc. v. Static Control Components, Inc., 2003 U.S. Dist. LEXIS 3734 (E.D. Ky. 2003).

[9] *See* The Chamberlain Group, Inc. v. Skylink Technologies, Inc., Civil Action No. 02c-6376 (N.D. Ill. Filed Sept. 6, 2002), http://www.eff.org/IP/DMCA/20030113_chamberlain_v_skylink_complaint.pdf; Pl.'s Am. Compl., *The Chamberlain Group, Inc.* (Oct. 16, 2002), http://www.eff.org/IP/DMCA/20030114_chamerberlain_v_skylink_amd_complaint.pdf; Pl.'s Mot. For Summ. J., *The Chamberlain Group, Inc.* (Dec. 3, 2002), http://www.eff.org/IP/DMCA/20030113_chamerlain_v_skylink_motion.pdf.

protection, which has narrower prohibitions, and (d) determining whether the function or market value of suspect software is primarily for circumvention or for its functionality. The following paragraphs elaborate on these difficulties, which are discussed in detail in the body of this Article; Table 1 summarizes their impact.

Table 1. Impact of DMCA Difficulties

Difficulty	Pre-DMCA Situation	Post-DMCA Impact
Separating expressive aspects of software from its functionality	Software covered by copyright but fair use exemptions apply Most expressive content restrictions against disclosure and discussion covered by First Amendment	? Prohibition against software implemented measures defeating copy and access protections ? Injunctions against software publication and release into public domain allowable because they are content neutral ? Limitations (unclear) against disclosure and discussion of technological measures
Defining the limits of acceptable reverse engineering	Reverse engineering and emulation of software OK if information not obtained by misappropriation	? Reverse engineering and emulation of copy and access protection measures prohibited except under limited circumstances ? Investigation into software operation (e.g., whether privacy related information released) prohibited except under limited circumstances
Distinguishing access from copy control	No issue	? Individual acting of Circumvention of copy control is protected in order to allow for fair use but not access control. If there is no distinction between the two activities, then both are effectively prohibited and scope of fair use is narrowed
Determining the primary purpose of a software package	No restriction on whether software could emulate "secret handshakes" or circumvent protection if no misappropriation	? Emulation of access control measures prohibited ? Definition of access control measures are very broad ? Emulation of non-access control functionality may be prohibited when not separable from access control functionality

? *Difficulty in separating expressive aspects of software from its functionality:* The expressive aspect of a computer program (and associated data structures) cannot be separated from its functionality. Software is written by persons who make conscious decisions concerning structure, algorithms, interfaces, design and implementation. Such decisions are recorded and documented in the source code when it is written, thereby constituting expression. Prior to the DMCA, courts held that software was a

literary work that contained expressive content and could be copyrighted under 17 U.S.C. 102(a).[10] However, like other copyrighted literary works, software could also be the subject of criticism or comment and made the object of scholarship and research under the fair use provisions of 17 U.S.C. § 107. Therefore, publishing criticisms on copy and access control, as well as distributing circumvention software was permissible (unless it was based on misappropriated information). Since the passage of the DMCA, courts have enjoined such software distribution, holding that section 1203 provisions allowing for injunctions against such activities are permissable because they are content-neutral restrictions on speech. The courts' view is that the *functionality* of circumvention measures rather than the expression of circumvention (which would be protected speech) is being enjoined. This view appears to be contrary to the holding of *Miller v. California*, the analogous Supreme Court case on pornography. The case established that lewd material with any literary or artistic value is protected by the First Amendment because it is not possible to separate the protected speech from the lewd content.[11]

? *Defining the limits of acceptable reverse engineering.* Prior to passage of the DMCA, reverse engineering of any software was permitted under the Uniform Trade

---

[10] Findings of Fact and Conclusions of Law, *Lexmark Int'l, Inc.*, 2003 U.S. Dist. LEXIS 3734 (E.D. Ky. Filed Feb. 27, 2003) ("A computer program, whether in object code or source code, is a 'literary work' and is protected from unauthorized copying, whether from the object or source code version", Apple Computer, Inc. v. Franklin Computer Corp., 714 F.2d 1240, 1249 (3d Cir. 1983)) *Available at* http://www.eff.org/Cases/Lexmark_v_Static_Controls/20030303-finding-of-facts.pdf (last visited Nov. 6, 2003). *See also* Feist Publ'ns, Inc. v. Rural Tel. Serv. Co. Inc., 499 U.S. 340 (1991). "The requisite level of creativity is extremely low; even a slight amount will suffice." *Id.* at 345. Indeed, "the vast majority of works make the grade quite easily, as they possess some creative spark, 'no matter how crude, humble or obvious' it might be." *Id.*

[11] Miller v. California, 413 U.S. 15, 26 (1973) ("…prurient, patently offensive depiction or description of sexual conduct [that has] serious literary, artistic, political, or scientific value [merits] First Amendment protection").

Secrets Act.[12] Thus, software written using the results of legitimate reverse engineering to emulate functionality or maintain file compatibility did not constitute infringement because it was not within the scope of copyright protection under 17 U.S.C. § 102(b).[13] However, the DMCA highly restricts reverse engineering[14] for copy or access control software. These restrictions assume that bright lines can be drawn around software components for which reverse engineering is allowed or prohibited. However, this is not always true. From the point of view of the copyright holder, a preferred software design may intermingle functional and protection routines in the same module. With such intermingling, it is difficult to characterize the nature of the integrated product as being a technical protection measure (which would be subject to DMCA restrictions) or functionality (which would not be subject to DMCA restrictions). As will be shown below, courts have found that software containing any protection measure would fall under the DMCA's anti-circumvention provisions. Moreover, software copyright owners can easily modify existing programs to incorporate copy or access control measures. They can then use the DMCA to enjoin the sale or distribution of any software that emulates their product or can read the files produced by their product by characterizing such emulation

---

[12] Uniform Trade Secrets Act With 1985 Amendments, § 1(2) and Prefatory Note *available at* http:www.law.upenn.edu/bll.ulc.fnact99/1980s/utsa85.htm (last visited Nov. 4, 2003) ("analysis involving the "reverse engineering" of a lawfully obtained product in order to discover a trade secret is permissible"). *See also* Wesley-Jessen, Inc., v. Reynolds, 182 USPQ 135, 144-45 (N.D. Ill. 1974) (unrestricted sale and lease of camera that could be reversed engineered in several days to reveal alleged trade secrets preclude relief for misappropriation).

[13] "In no case does copyright protection for an original work of authorship extend to any *idea, procedure, process, system, method of operation, concept, principle, or discovery,* regardless of the form in which it is described, explained, illustrated, or embodied in such work." 17 U.S.C. § 102(b) (2003) (emphasis added).

[14] 17 U.S.C. § 1201(f) (2003).

programs as circumvention. The net result is to inhibit competition from "clone" programs and after-market compatible products (such as printer toner cartridges) to preserve monopolies.

? *Difficulty of distinguishing access control circumvention from copy control circumvention:* Access and copy control are distinguishable in the analog domain of cable and satellite television signals (from which it appears that these two concepts were derived). However, it is not possible to readily distinguish access from copy control in the digital domain of files and bit streams that can be stored and processed as files. Section 1201 has separate subsections to address access and copy control circumvention, and the two prohibitions are different: Persons are prohibited from *engaging* or *trafficking* in access control circumvention measures, but only from *trafficking* in copy control circumvention.

? *Difficulty of determining whether software has been written "primarily" to circumvent a protection measure.* Congress assumed that software could be readily categorized as being "primarily"[15] a circumvention method or whether its primary market value lay in its functionality. However, it is unclear how fact-finders should make this determination. Traditional product measures such as material composition or manufacturing cost do not apply to software. In the *Streambox* and *Skylink* cases discussed below, the courts held that *any* circumvention technology included in a large multifunctional program renders that program as being in violation of the DMCA's anti-circumvention provisions.

[15] *See, e.g.,* 17 U.S.C. § 1201(a)(2) and § 1201(b)(1) (2003) ("primarily designed or produced for the purpose of circumventing…a technological measure").

These points are discussed in greater detail below. Section II provides an overview of the DMCA anti-circumvention provisions. Section III contains a discussion of the issues listed in Table 1, and Section IV concludes with recommendations on changes to the DMCA that will address these problems.

II. Statutory Overview

This part of the Article provides an overview of sections 1201, 1203, and 1204 of the U.S. Copyright Act. The first subdivision describes the anti-circumvention prohibitions as defined in the act, the second identifies the remedies, and the third discusses the applicable exemptions, i.e., anti-circumvention "safe harbors."

A. Anti-circumvention Prohibitions

Section 1201 contains three major anti-circumvention prohibitions:[16]

1. *Acting* to circumvent *access control*: Section 1201(a)(1)(A) prohibits a person from circumventing a "technological measure that effectively controls access to a work protected under this title." A "technological measure that effectively controls access" is defined as a mechanism which "in the ordinary course of its operation, requires the application of information, or a process or a treatment, with the authority of the copyright owner, to gain access to the work."[17] The definition of access control circumvention is "to descramble a scrambled work, to

[16] The term "anti-circumvention provisions" is used in same manner in which it is used by the the Second Circuit. *See*, Universal City Studios, Inc., v. Corley, 273 F.3d 429, 435 (2d Cir. 2001).

[17] 17 U.S.C. § 1201(a)(3)(B).

decrypt an encrypted work, or otherwise to avoid, bypass, remove, deactivate, or impair a technological measure, without the authority of the copyright owner."[18]

2. *Trafficking in technologies or devices* that circumvent *access control:* Section 1201(a)(2) prohibits the manufacture, importing, offering to the public, providing, or otherwise trafficking in technology or products primarily designed or produced to circumvent a "technological measure that effectively controls access to a work protected under this title." The definitions of technological measures and circumvention of access control are the same as those in the previous paragraph.

3. *Trafficking in technologies or devices* that circumvent *rights protection: Section* 1201(b)(1) prohibits the manufacture, importing, offering to the public, providing, or otherwise trafficking in technology or products primarily designed or produced to circumvent a technological measure that effectively protects a right (i.e., the reproduction right) of a copyright owner. A "technological measure that effectively protects a right of a copyright owner " is defined as a mechanism which "in the ordinary course of its operation, prevents, restricts, or otherwise limits the exercise of a right of a copyright owner."[19] Because copying is the dominant right to be protected, in this Article, the term "copy protection" is used to refer to this subsection. Circumvention is defined as "avoiding, bypassing, removing, deactivating, or otherwise impairing a technological measure."[20]

The three prohibitions can be characterized in two dimensions: (1) as "acting" and "trafficking" prohibitions, and (2) as "access control" and "rights or copy control"

---

[18] 17 U.S.C. § 1201(a)(3)(A).

[19] 17 U.S.C. § 1201(b)(2)(B).

circumvention prohibitions. Table 2 shows a conceptual framework for this categorization.

Table 2. DMCA Anti-circumvention Provisions

Prohibitions	Access control	Copy (i.e., "Rights") protection
Acts of Circumvention	1201(a)(1)(A)	None
Trafficking in circumvention tools and technologies	1201(a)(2)	1201(b)(1)

The conditions of the anti-trafficking provisions 1201(a)(2) and 1201(b)(1) that subject a defendant to liability are that the device or technology

? is primarily designed or produced for the purpose of circumventing a technological measure that effectively controls access to a system protected by a registered copyright or effectively protects a right of a copyright owner in a registered work (or portion)

? has only limited commercially significant purpose or use other than to circumvent such a technological measure (or protection afforded it); or

? is marketed for use in circumventing such a technological measure.[21]

Congress also sought to balance these circumvention prohibitions by protecting fair use. However, courts have interpreted this language in a very restricted manner. Thus, subsection 1201(c)(1) states that "[n]othing in this section shall affect rights, remedies, limitations or defenses to copyright infringement, including fair use, under this title." Courts have interpreted this section to apply only to the copyrighted material itself, not to the copy and access protection measures, to information on how to circumvent the

[20] 17 U.S.C. § 1201(b)(2)(A).

[21] 17 U.S.C. §§ 1201(a)(2)-(3), (b)(1)-(2).

measures, or to links to Internet sites that provide such descriptions.[22] Similarly, subsection 1201(c)(4), which provides that "[n]othing in this section shall enlarge or diminish any rights of free speech or the press for activities using consumer electronics, telecommunications, or computing products" and which could have been interpreted as protecting a discussion of copy and access protection measures under the First Amendment, has been interpreted as being "clearly precatory."[23]

B. Remedies

17 U.S.C. § 1203 allows persons injured by violations of section 1201 to bring civil actions in federal district courts. The district courts are given the power to grant temporary or permanent injunctions, impound devices, award damages, allow for the recovery of costs and attorney's fees, and order the remedial modification or destruction of offending devices.

17 U.S.C. § 1204 defines a criminal offense for any person who willfully violates section 1201 for the purposes of commercial advantage or private gain.

C. Exemptions

The DMCA has provided limited exemptions to the anti-circumvention prohibitions discussed above. The "safe harbors" are reverse engineering[24], encryption research,[25] security testing,[26] and protection of personally identifying information.[27]

---

[22] *Corley*, 273 F.3d at 443, "[S]ubsection 1201(c)(1) ….simply clarifies that the DMCA targets the circumvention of digital walls guarding copyrighted material (and trafficking in circumvention tools), but does not concern itself with the use of those materials after circumvention has occurred."

[23] *Id.* at 444, "Congress could not "diminish" constitutional rights of free speech even if it wished to, and the fact that Congress also expressed a reluctance to "enlarge" those rights cuts against the Appellants' effort to infer a narrowing construction of the Act from this provision."

[24] 17 U.S.C. § 1201(f).

1. Reverse Engineering

The reverse engineering exemption allows the circumvention of copy and access control under four restrictive conditions

- The person performing the reverse engineering has lawfully obtained the right to use a copy of a computer program;
- Access control may be circumvented for the sole purpose of identifying those elements of the program (i.e., software components) required for interoperability (i.e., software or hardware interfacing) with an independently written program;
- The interfaces and other information required for interoperability are not readily available to the person engaging in the circumvention; and
- The acts of identification and analysis do not constitute infringement.[28]

The reverse engineering results and circumvention methods permitted under the above conditions may be made available to others " [1] solely for the purpose of enabling interoperability of an independently created computer program with other programs, and [2] to the extent that doing so does not constitute infringement under this title or violate applicable law other than this section [1201]."[29] Any other disclosure would be a violation of the DMCA. This exemption would not allow a general discussion of the

---

[25] 17 U.S.C. § 1201(g).

[26] 17 U.S.C. § 1201(j).

[27] 17 U.S.C. § 1201(i).

[28] 17 U.S.C. § 1201(f)(1)-(2).

[29] 17 U.S.C. § 1201(f)(3).

results of reverse engineering of software, and would not apply at all to hardware implemented copy or access protection.[30]

2. Encryption Research

The exemption for encryption research requires that the person establish that circumvention is necessary to conduct such encryption research, obtain authorization before the circumvention; not disseminate the results in a manner that would facilitate infringement; and engage in a "legitimate" course of study or be "appropriately trained or experienced" in cryptology. The results of the research may be passed only to other collaborators for "good-faith" encryption research or to have the work verified. They may not be passed to a normal computer user.

3. Security Testing

Under the security testing exemption of the DMCA, a person may engage in security testing (including using circumvention measures to defeat access control provisions[31]) if the information derived from the security testing was used to promote the security of the system or network under test or shared only directly with the developer of such a system.[32] Thus, sharing the results of such testing with a wider audience would be a violation of the anti-trafficking provisions.

---

[30] One can only speculate as to whether a firmware protection measure would be considered hardware or software.

[31] 17 U.S.C. §1201(j)(4) (2003) ("Use of technological means for security testing. Notwithstanding the provisions of subsection (a)(2), it is not a violation of that subsection for a person to develop, produce, distribute or employ technological means for the sole purpose of performing the acts of security testing described in subsection (2), provided such technological means does not otherwise violate section (a)(2).").

[32] 17 U.S.C. §1201(j)(2)(B) (2003) ("[W]hether the information derived from the security testing was used or maintained in a manner that does not facilitate infringement under this title or a violation of applicable law other than this section, including a violation of privacy or breach of security.").

4. Dissemination of Personal Information

Perhaps the most problematic circumvention exemption is 1201(j), which allows circumvention of access controls that disseminate personally identifying information or online activities. The act of circumvention must be solely for the purpose of preventing the collection or dissemination of personally identifying information; it does not apply to a technological measure that does not collect or disseminate personally identifying information. On the one hand, this category of exemption might be the most relevant because an increasing number of software packages require "activation" after installation.[33] However, because the details of such measures are not likely to be published by the copyright owners, it is only possible for persons to know whether the circumvention qualifies for the exemption after they have circumvented the access or copy control and determined if it is transmitting personal information. Other requirements are that the act of circumvention have the sole effect of identifying and disabling the capability described in subparagraph 1201(j), and that it have no other effect on the ability of any person to gain access to any work.

III. Discussion

This part analyzes significant cases related to section 1201 and explains how they relate to the issues raised in the introduction. The first section addresses the difficulty of separating expressive aspects of software from its functionality, the second describes the uncertainties introduced by the DMCA in limits of acceptable reverse engineering, the third discusses the difficulties in distinguishing access from copy control, and the final

[33] *See,* e.g., Microsoft Product Activation, *at* http://www.microsoft.com/piracy/basics/activation/ (posted Dec. 8, 2003).

section addresses the problems in determining the primary purpose of a software package for the purposes of determining whether it violates the anti-trafficking provisions of subsections 1201 (a)(1)(A), 1201 (a)(2), and 1201 (b) .

A. Difficulty of Separating Expressive and Functional Aspects of Software

Courts have issued and upheld injunctions on posting, publishing, or otherwise distributing software that they found violated the anti-circumvention sections of the DMCA, explaining that while computer programs are protected speech,[34] the fact that they are executable also gives them a functional aspect. Thus, such injunctions are content-neutral restrictions on speech that are subject to an intermediate standard of judicial review.[35] Furthermore, because links leading to other web sites from which offending programs can be downloaded can be traversed with "the click of a mouse," even such links can be subject to an injunction under the DMCA.[36]

In *Universal City Studios, Inc. v. Reimerdes*,[37] eight motion picture studios sought an injunction under 17 U.S.C. § 1203(b)(1) to prevent *2600 Magazine* from publishing or

---

[34] *See, e.g.*, Universal City Studios v. Corley, 273 F.3d 429, 449 (2d Cir. 2001) ("[W]e join the other courts that have concluded that computer code, and computer programs constructed from code can merit First Amendment protection.").

[35] *See, e.g.*, Universal City Studios, Inc. v. Reimerdes, 111 F. Supp. 2d 294, 329 (S.D.N.Y. 2000), *judgment entered*, 111 F. Supp. 2d 346 (S.D.N.Y. 2000), *aff'd on other grounds, sub nom* Universal Studios, Inc. v. Corley, 273 F.3d 429 (2d Cir. 2001), ("As Congress' concerns in enacting the anti-trafficking provision of the DMCA were to suppress copyright piracy and infringement and to promote the availability of copyrighted works in digital form, and not to regulate the expression of ideas that might be inherent in particular anti-circumvention devices or technology, this provision of the statute properly is viewed as content neutral.").

[36] *Id.* at 341 ("A copyright holder may seek an injunction to remove links when there is "clear and convincing evidence that those responsible for the link (a) know at the relevant time that the offending material is on the linked-to site, (b) know that it is circumvention technology that may not lawfully be offered, and (c) create or maintain the link for the purpose of disseminating that technology.").

[37] *See surpa* note 35 for procedural history.

linking to DeCSS, a software-implemented circumvention mechanism that defeated an encryption mechanism called the "Content Scrambling System" (CSS) managed by the Digital Video Disk Copy Control Association (DVD CCA). The court stated that

> the anti-trafficking provision of the DMCA as applied to the posting of computer code that circumvents measures that control access to copyrighted works in digital form is a valid exercise of Congress' authority. It is a content neutral regulation in furtherance of important governmental interests that does not unduly restrict expressive activities.[38]

In granting the injunction, the court rejected the argument of the defendants that the DMCA violates the First Amendment: The court reasoned that the DeCSS source code was composed of both functional and speech elements, but that the functional elements predominated, stating that

> [t]he presence of some expressive content in the [source or object] code should not obscure the fact of its predominant functional character--it is first and foremost a means of causing a machine with which it is used to perform particular tasks.[39]

The court then held that restrictions on the functional elements are content neutral[40] and therefore subject to intermediate scrutiny. Using that standard, the court found that the value of the free expression of decryption ideas was outweighed by the government's interest in preventing infringement and promoting the availability of content in a digital form, and there was an imminent threat of danger flowing from the dissemination of the software that far outweighed the need for the unfettered

---

[38] *Id* at 332.

[39] *Id* at 335.

[40] *Id* at 329 ("The reason that Congress enacted the anti-trafficking provision of the DMCA had… to do with functionality--with preventing people from circumventing technological access control measures…[I]t is focused squarely upon the effect of the distribution of the functional capability that the code provides. Any impact on the dissemination of programmers' ideas is purely incidental to the overriding concerns of promoting the distribution of copyrighted works in digital form while at the same time protecting those works from piracy and other violations of the exclusive rights of copyright holders.").

communication of that software.[41] Section 1203(a), which allows "any person injured by a violation of section 1201 or 1202" to "bring a civil action in an appropriate United States court for such violation" was then upheld by the court.

In *United States v. Elcom Ltd.*,[42] the court affirmed the constitutionality of DMCA in a criminal prosecution using slightly different reasoning. The defendant was a Russian software company that marketed a product that enabled users to access password - rotected files and in particular, the digital rights management provisions of Adobe E- books files.[43] The defendant moved to dismiss the charges on first amendment grounds.[44] As was the case in *Reimerdes,* the court rejected the defendant's arguments that the anti-circumvention prohibition of 17 U.S.C. § 1201(b) constituted a content-based restriction on speech. However, in contrast to the speech/functionality duality of software, the court analogized the *criminal* DMCA prohibitions to content neutral restrictions on expressive conduct, stating that "[w]hen speech and non-speech elements are combined in a single course of conduct, a sufficiently important government interest in regulating the non-speech element can justify incidental intrusions on First Amendment freedoms."[45] Once content neutrality was established, the court used the intermediate scrutiny standard, i.e., legitimate government interests that did not burden substantially more speech than was

---

[41] *Id*. at 339.

[42] United States v. Elcom Ltd., 203 F. Supp. 2d 1111 (2002)

[43] E-books are the name given by Adobe Software Corporation to its variant of widely used Acrobat files that are integrated with rights management cont rols for access, copying, redistribution, printing, and other reproduction methods.

[44] *Elcom*, 203 F. Supp. 2d. at 1121.

[45] *Id*. at 1127-28, *citing* United States v. O'Brien, 391 U.S. 367 (1968) (rejecting defendant's argument that regulation against burning of draft card was unconstitutional because it was enacted to abridge free speech, instead holding that regulation served legitimate legislative purpose not related to speech); Junger v. Daley, 209 F.3d 481, 485 (6th Cir. 2000) (applying intermediate scrut iny to regulations banning exportation of encryption software).

necessary to achieve those interests, and found that the DMCA anti-circumvention prohibitions met that standard.[46] At the trial, the jury found Elcom not guilty because it had not knowingly violated section 1201(b). This outcome is fact-specific. Charges could still be brought against defendants who "traffick in" similar software. Not surprisingly, Russia has issued a travel advisory to Russian programmers traveling in the United States.[47]

The "code-as-function" view of *Reimerdes* had an effect on trade secret law as well. In *DVD Copy Control Assn v. Bunner,*[48] the California Supreme Court affirmed a preliminary injunction against the posting of DeCSS holding that the injunction was a content-neutral regulation of speech relying in part on the conclusions of *Reimerdes*. The DVD CCA brought an action under the California version of the Uniform Trade Secrets Act (UTSA) against Andrew Bunner and several other defendants who had allegedly published or linked to DeCSS. The court held that under the UTSA, the purpose of the injunction is to prevent disclosure of a trade secret, and the injunction was made independent of the content of the posting.[49] The court remanded for further consideration the question whether in fact the DeCSS code was the result of a misappropriated trade secret under the UTSA.

---

[46] The *Elcom* Court also rejected the defendant's vagueness argument because it did not describe what speech it prohibits (and therefore, Congress had exceeded its powers in passing the law). *Elcom*, 203 F. Supp. 2d at 1125. The court held that section 1201(b) was not unconstitutionally vague as applied to the software company because it allowed a person to conform his or her conduct to a comprehensible standard. *Id.* The court further held that the governmental interests in enacting the DMCA were both legitimate and substantial and did not burden substantially more speech than was necessary to achieve those interests. *Id.* at 1131-32. Finally, the court finally held that the DMCA was not facially unconstitutionally vague, and did not exceed U.S. Congressional power. *Id*. at 1141-42.

[47] Jennifer 8 Lee, *Travel Advisory for Russian Programmers*, N.Y. TIMES, Sept.10, 2001, at C4, *available at* http://www.nytimes.com/2001/09/10/technology/10WARN.html?searchpv=past7days.

[48] DVD Copy Control Assn v. Bunner, 31 Cal. 4th 864 (2003),

Bunner suggests a way that a copyright holder can use the UTSA synergistically with the DMCA anti-trafficking prohibition to suppress *any* discussion or description of how to circumvent copy or access control (i.e., even if the discussion is not expressed as compilable high level source code or executable object code).[50] A posting of the code on an unrestricted web site or other publication of the results of a reverse engineering activity on an access or copy control measure would fall outside of the reverse engineering exemption of section 1201(f). Thus, persons referencing (by means of a link or other mechanism) or material that described how to circumvent or interface with a protection measure would have or should have known that such material was illegally published or disclosed and hence, they acquired the information by improper means.[51] Therefore, such individuals would be liable for misappropriation,[52] and the posting of such instructions can be enjoined under the UTSA.[53]

The net result of these decisions is a general uncertainty as to what discussion of computer security, access protection, and copy control is allowed within the scope of the DMCA and conversely, the limits of first amendment protections. Two clearly apparent effects have been in the areas of academic research on computer security and the limitation on property rights of computer and network owners and users.

---

[49] *Id.* at 12.

[50] Neither *Reimerdes* nor *Elcom* address the question of whether expressive content that describes and criticizes circumvention methods without necessarily reducing them to code is a violation of the anti-circumvention provisions.

[51] CAL. CIV. CODE §3426.1 (West, WESTLAW through 2004 Legis. Sess.) ("As used in this title, unless the context requires otherwise (a) "Improper means" includes …breach of a duty to maintain secrecy . . . .").

[52] *Id.* ("(b) 'Misappropriation' means (1) Acquisition of a trade secret of another by a person who knows or has reason to know that the trade secret was acquired by improper means . . . .").

[53] CAL. CIV. CODE §3426.2(a) (West, WESTLAW through 2004 Legis. Sess.) ("Actual or threatened misappropriation [of a trade secret] may be enjoined.").

1. Chilling of Speech in Academic Research on Computer Security

Section 1201 of the DMCA has impacted the free exchange of ideas in the area of academic research on computer security. For example, the Recording Industry Association of America (RIAA) threatened civil *and criminal* prosecution against Professor Edward Felten of Princeton University if he did not withdraw a paper at a computer conference called the Information Hiding Workshop. The paper topic was his success in breaking the Secure Digital Music Initiative (SDMI) encryption code in response to an RIAA publicly announced challenge to security researchers. The RIAA letter to Felten stated that

> public disclosure of your research would be outside the limited authorization of the Agreement [concerning an RIAA Public Challenge to "break" the SDMI code], *you could be subject to enforcement actions under federal law, including the DMCA*. The Agreement specifically reserves any rights that proponents of the technology being attacked may have 'under any applicable law, including, without limitation, the U.S. Digital Millennium Copyright Act, for any acts not expressly authorized by their Agreement.' The Agreement simply does not 'expressly authorize' participants to disclose information and research developed through participating in the Public challenge and such *disclosure could be the subject of a DMCA action*. [emphasis added][54]

Felten withdrew his paper from the conference and posted a response which stated in part that

> the Recording Industry Association of America, the SDMI Foundation, and the Verance Corporation threatened to bring a lawsuit if we proceeded with our presentation or the publication of our paper. Threats were made against the authors, against the conference organizers, and against their respective employers.[55]

---

[54] Letter from Matthew J. Oppenheim, Esq. to Edward Felten, Department of Computer Science Princeton University (Apr. 9, 2001), *available at* http://cryptome.org/sdmi-attack.htm (lasted visited Dec. 8, 2002).

[55] Statement by Edward W. Felten, Fourth International Information Hiding Workshop, Pittsburgh, PA (Apr. 26, 2001), *available at* http://cryptome.org/sdmi-attack.htm (last visited Nov. 8, 2003).

Not surprisingly, the International Information Hiding Workshop Conference has chosen to hold all of its future conferences outside of the U.S.[56]

A loosely organized collective known as Secure Network Operations ("SNOsoft"), received a similar DMCA warning letter after releasing software in July 2002 that demonstrated vulnerabilities in the Hewlett Packard (HP) Tru64 UNIX operating system. This had an impact on the group even though HP ultimately withdrew the threat.[57]

Other computer security experts have curtailed their research activities out of fear of potential DMCA liability. For example, Neils Ferguson, a prominent Dutch cryptographer and security systems analyst discovered a major security flaw in an Intel video encryption system known as High Bandwidth Digital Content Protection (HDCP). He declined to publish his results and removed all references on his website relating to flaws in HDCP, on the grounds that he travels frequently to the U.S. and is fearful of "prosecution and/or liability under the U.S. DMCA law."[58] British computer scientist Alan Cox has urged USENIX, a major operating system organization, to hold its annual conference outside of the United States.[59] Another network security protection

---

[56] Will Knight, *Computer Scientists Boycott US Over Digital Copyright Law*, NEW SCIENTIST (July 23, 2001), http://www.newscientist.com/news/news.jsp?id=ns00001063.

[57] Declan McCullagh, *Security Warning Draws DMCA Threat*, CNET NEWS (July 30, 2002), *at* http://news.com.com/2100-1023-947325.html.

[58] *See* Neils Ferguson, *Censorship in Action: Why I Don't Publish My HDCP Results*, *at* http://www.macfergus.com/niels/dmca/cia.html (Aug. 15, 2001); *see also* Neils Ferguson, Declaration in Felten & Ors v R.I.A.A. case Aug. 13, 2001, *available at* http://www.eff.org/IP/DMCA/Felten_v_RIAA/20010813_ferguson_decl.html (last visited Nov. 8, 2003); Lisa M. Bowman, *Researchers Weigh Publication, Prosecution*, CNET NEWS (Aug. 15, 2001), *at* http://news.cnet.com/news/0-1005-200-6886574.html.

[59] Alan Cox of Red Hat UK Ltd, Declaration in Felten & Ors v RIAA, Aug. 13, 2001, *available at* http://www.eff.org/IP/DMCA/Felten_v_RIAA/20010813_cox_decl.html.

researcher, Dug Song, also removed a paper describing a common vulnerability in many firewalls from his website for fear of prosecution–even though it had nothing to do with the DMCA.[60] In mid-2001, an anonymous programmer discovered a vulnerability in Microsoft's proprietary e-Book digital rights management code, but refused to publish the results, citing DMCA liability concerns.[61]

The Institute of Electrical and Electronic Engineers (IEEE) is one of the largest engineering societies in the world and publishes about 30 percent of the technical journals in the United States. In response to concerns about potential liability of the DMCA, the IEEE in November 2001 instituted a policy requiring all authors to indemnify the Institute for any liabilities incurred should a submission result in legal action under the DMCA. The organization ultimately revised its submission policies, removing mention but the chill remains, as reflected in the following IEEE statement.

> Among its provisions, DMCA prohibits 'any technology, product, service, device component or part' that circumvents digital copy protection systems. This has been perceived as a serious problem, by scientists and engineers who fear that this could prevent them from even publishing articles about digital protection, encryption, or cryptography technologies.[62]

According to an IEEE press release, "The Digital Millennium Copyright Act has become a very sensitive subject among our authors. It's intended to protect digital

---

[60] Robert Lemos, *Security Workers: Copyright Law Stifles*, CNET NEWS (Sept. 6, 2001), *at* http://news.com.com/2100-1001-272716.html.

[61] Wade Roush, *Breaking Microsoft's e-Book Code*, TECH. REV., Nov. 2001, at 24, *available at* http://www.technologyreview.com/articles/innovation11101.asp.

[62] Press release, IEEE, IEEE to Revise New Copyright Form to Address Author Concerns (Apr. 22, 2002). *available at* http://www.ieee.org/newsinfo/dmca.html.

content, but its application in some specific cases appears to have alienated large segments of the research community."[63]

In a column in *PC Magazine,* a widely read general technical interest publication, John Dvorak, a well-known writer and commentator on the PC industry wrote:

> How long will it be before a college professor is busted for a frank discussion about code? Will there be a way for the industry itself to have meetings where such issues are discussed? Am I breaking some aspect of the DMCA law by writing this column? Maybe. Where does it end? Should everyone think twice before they say anything? Folks, this [sic] is the roots of fascism, plain and simple.[64]

2. Limitation on Property Rights of Computer and Network Owners

Because of the uncertain breadth of the anti-trafficking prohibitions and the narrowness of the exemptions, the DMCA effectively prohibits owners of systems and equipment from knowing how their systems operate. Thus, the DMCA is interfering with a basic property right, i.e., an owner's ability to know of what the item is composed and how it works. In the case of software implemented access and copy control measures, these anti-trafficking sections prevent owners of personal computers from knowledge of how their systems work, what changes have been made to their system registries and file systems, and what information is being transmitted to the owners of copyrighted material packaged with such controls. This prohibition extends not only to private users of personal computers but also to public agencies.

A consequence of this prohibition is interference with not only private owners but also public agencies in verifying the security of their systems and the extent to which

---

[63] *Id.*

the privacy of citizens is at risk. For example, because of the highly restrictive nature of the personal information exemption in section 1201(j), a county election registrar might not be able to hire an expert to evaluate a computer-based voting system to ensure that its security measures do not capture information on how individual voters voted and that the information would not be transmitted to a third source (e.g., a news or polling organization).

B. Difficulty in Defining the Limits of Acceptable Reverse Engineering

Reverse engineering is defined as "starting with a known product and working backward to divine the process which aided in its development and manufacture."[65] Courts have held that reverse engineering of a trade secret contained in a legitimately purchased or otherwise acquired product is not misappropriation.[66] Under the UTSA[67] and similar statutes (passed by most states), persons are liable for use or disclosure of misappropriated trade secrets. In the case of software, courts have sanctioned reverse engineering when there was no misappropriation of trade secrets and if the resulting product was not infringing. In *Sega Enterprises Ltd. v. Accolade, Inc.*[68] the court held that where disassembly or intermediate copying is the only way to gain access to the

---

[64] John C. Dvorak, *The Sklyarov Gambit*, PC MAGAZINE, July 23, 2001, *available at* http://www.pcmag.com/article2/0,4149,25446,00.asp (last visited March 6, 2004).

[65] ROBERT P. MERGES, PETER S. MENELL, AND MARK A. LEMLEY, INTELLECTUAL PROPERTY IN THE NEW TECHNOLOGICAL AGE, 989 (Aspen Publishers 2000).

[66] See, e.g., Wesley-Jessen, Inc. , *supra* note 12 (unrestricted sale and lease of camera that could be reverse engineered in several days to reveal alleged trade secrets preclude relief for misappropriation). *See also* Prefatory Notes to the Universal Trade Secrets Act with 1985 Amendments, *supra* note 12 ("analysis involving the 'reverse engineering' of a lawfully obtained product in order to discover a trade secret is permissible.").

[67] Universal Trade Secrets Act Section 1(2), *supra* note 12.

[68] Sega Enterprises Ltd. v. Accolade, Inc., 977 F.2d 1510, 1527-28 (9th Cir. 1993) (amended opinion).

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.

In *Sony Computer Entertainment, Inc. v. Connectix Corp.*, the court held that making intermediate copies of object code while performing reverse engineering activities in order to emulate another software product is fair use. [69] The defendant, Connectix Corporation, developed a software product called the "Virtual Game Station" that emulated the functionality of the Sony PlayStation console (a computer manufactured and marketed for the purposes of running video games) on a conventional personal computer. Although the Virtual Game Station did not contain any of Sony's copyrighted material, Sony claimed infringement because Connectix repeatedly copied Sony's copyrighted BIOS while reverse engineering its interfaces and functions. The district court concluded that Sony was likely to succeed on its infringement claim because Connectix's intermediate copying was not a protected fair use. The appellate court reversed the lower court and dissolved the injunction, holding that the copies made by Connectix in the course of the reverse engineering process did constitute fair use.[70] The court adopted the holding of *Sega v. Accolade.* In its decision, the court stated that as an alternate platform for executing Playstation computer games, "the Virtual Game Station is a legitimate competitor in the market for platforms on which Sony and Sony-

[69] Sony Computer Entertainment, Inc. v. Connectix Corp., 203 F.3d 596, 611 (9th Cir., 2000)

[70] *Id.* at 599. ("Software engineers designing a product that must be compatible with a copyrighted product frequently must 'reverse engineer' the copyrighted product to gain access to the functional elements of the copyrighted product. Software engineering …methods… require that the person seeking access load the target program on to a computer, an operation that necessarily involves copying the copyrighted program into the computer's random access memory or RAM").

licensed games can be played."[71] This result is in marked contrast to that of the *Reimerdes* court, which enjoined reverse engineering and the posting of results of reverse engineering (even when not for a commercial advantage) because the CSS was entitled to the status of a "technological measure" under the DMCA.

As noted above, under the DMCA, reverse engineering activities are highly proscribed, and courts have upheld these restrictions. In *Reimerdes,* the court rejected on three grounds the defendant's argument that DeCSS was written as part of a reverse engineering process for creating a DVD player that would run on the Linux operating system. First, the defendants did not actually perform the reverse engineering: they posted the results of others' work. Second,, even if they had authored DeCSS, the right to make the information available was provided "solely for the purpose" of achieving interoperability as defined in the statute. It does not apply to public dissemination of means of circumvention. The court found that "These defendants, however, did not post DeCSS 'solely' to achieve interoperability with Linux or anything else."[72] Finally, because DeCSS ran on the Microsoft Windows operating system, the court rejected the assertion that DeCSS was not written solely for the purposes of developing DVD Playing software for the Linux operating system.

Because of the changeable nature of software, the exponentially increasing processing and storage capacity of hardware, the decreasing cost of high-speed communication, and the introduction of new technologies such as broadband wireless, digital technology is constantly evolving. The ability to reverse engineer is therefore

---

[71] *Id.* at 607.

[72] *Reimerdes*, 111 F. Supp. 2d at 320.

essential to ensure downward compatibility and smooth migrations. By way of example, all of the opinions described above were written on personal computers containing firmware called a BIOS (Basic Input/Output System) that was reverse engineered from the original created by IBM Corporation for the IBM PC. Had the BIOS been considered a "technological measure" under the DMCA, the reverse engineering would have been prohibited under the DMCA because if IBM were to have licensed the BIOS, the condition described in section 1201(f) ("not readily available to the person engaging in the circumvention") would have not been met, and IBM could have obtained an injunction to prevent the development of IBM PC compatible "clones."

C. Difficulty in Distinguishing Access from Copy Control

The DMCA anti-circumvention provisions discussed above distinguish between *access control* and *rights protection*. Access control was intended by Congress to be "the electronic equivalent of breaking into a locked room in order to obtain a copy of a book"[73] whereas copy control (as well as other rights control measures) relates to the actual act of reproduction, distribution, or other rights (defined in 17 U.S.C. § 106). The model is suitable for satellite and Cable TV descramblers, in which the access was the act of descrambling the broadcast (or cable) signal (and is not a violation of copyright law) and the copying was the actual recording and reproduction of the broadcast content.[74]

However, when the technical measures are implemented in software (or firmware) and operate on persistent data storage (e.g., a file or a Digital Video Disk) containing

---

[73] H.R. REP. No. 105-551, pt. 1, at 17 (1998).

[74] Jonathan Weinberg, *Digital TV, Copy Control, and Public Policy*, 20 CARDOZO ARTS & ENT. L.J. 277 (2002).

encrypted content or encrypted streaming data (which is a modified form of file transfer) rather than a transient scrambled broadcast signal, the distinction between access control and copy control vanishes. The circumvention occurs by processing the encrypted content to create a second file that contains non-encrypted content. For example, the Content Scrambling System (CSS) used on all Digital Video Disks (DVDs) with motion picture content to prevent unauthorized duplication is managed by the DVD *Copy Control* Association [emphasis added]. Under the definition laid out in section 1201(b)(2)(B), CSS should be considered a rights (i.e., copy) control technological measure because it "effectively protects a right of a copyright owner." Moreover, by virtue of having physical possession of the DVD, a person has access to the content. Nevertheless, section 1201(a)(3)(B) explicitly defines content encryption as being an access control measure. Thus, in *Reimerdes* the court categorized DeCSS, a program that defeated CSS, as circumventing an *access control* rather than a *copy control* measure.[75]

Another example of the confusion can be seen in *Realnetworks, Inc. v. Streambox, Inc.*,[76] 2000 U.S. Dist. LEXIS 1889 (W.D. Wa. 1999). The court granted an injunction against distributing Streambox VCR, a digital video and audio software file player that emulated the Real Networks Realplayer, a parallel product created by the plaintiff. In granting the injunction, the court held that the defendant was likely to be found to violate DMCA sections 1201(a)(2) *and* 1201(b), because the Streambox player could emulate a "secret handshake" communication protocol which could allow a permanent copy of a

[75] *Reimerdes*, 111 F.Supp.2d at 316.

[76] Realnetworks, Inc. v. Streambox, Inc., 2000 U.S. Dist. LEXIS 1889 (W.D. Wa. 1999).

file to be stored on the user's machine.[77] The Realplayer "secret handshake" (a protocol in which authentication information was exchanged between the sender and receiver of copyrighted files) would appear to be more of an access control rather than a copy control measure because failure of the handshake would result in a denial of access to the content. However, the court found that that "… at least a part of the Streambox VCR is primarily, if not exclusively, designed to circumvent *the access control and copy protection* measures that RealNetworks affords to copyright owners."[78] The court held that "the [offending Streambox product] circumvents the Secret Handshake so as to avoid the Copy Switch has no significant commercial purpose other than to enable users to *access and record protected content*"[79] From this holding, one can infer that the court based its combined access and copy control circumvention classification on the *result* of the circumvention (enabling a copyrighted file to be duplicated on the user's computer) as well as the *means* by which it occurred.

On the other hand, some courts have been more definite in their characterization. In *Sony Computer Entertainment America, Inc. v. Gamemasters,*[80] the court granted a preliminary injunction to the plaintiff holding that the Game Enhancer circumvented *access* control measures. The defendant marketed a firmware-based device called a game

---

[77] A feature of the Realserver/Realplayer combination was the "copy switch" which either allowed or prevented the streamed data from the server to be permanently stored on the file. By means of streaming and a disabled copy switch, copyright holders could allow users to download and view their content in digital form but prevent them from storing the data in permanently a file on their client machines. The Streambox VCR, on the other hand, allowed users to override the copy switch and store the audio and video data irrespective of the switch setting.

[78] *Streambox*, 2000 U.S. Dist. LEXIS 1889 at 20-21.

[79] *Id.* (emphasis added). A condition for liability under 1201(a)(2)(B) and 1201(b)1(B) is that the circumvention measures not have any other commercially significant purpose.

[80] Sony Computer Entertainment America v. Gamemasters, 87 F. Supp. 2d 976 (N.D. Cal. 1999).

enhancer that circumvented a measure on a Sony Playstation that authenticated CD-ROMs by means of a code contained on authorized copies. However, even here, there is a variation that was not necessarily anticipated by the original drafters of the DMCA: it is not the copyrighted CD itself for which the circumvention was enjoined. The court's perspective on this protection measure was that access control to the (copyrighted) firmware on the *game device* was the item that was being circumvented by the (presumably infringing unauthorized copy) *CD-ROM* .

The same perspective was taken in *Lexmark Int'l, Inc. v. Static Control Components, Inc.*.[81] The defendant produced components for remanufactured printer and toner cartridges for laser printers made by Lexmark, a leading printer manufacturer. The cartridges came in two varieties: refillable and non-refillable. Static Controls (SCC) developed components to enable the non-refillable cartridges to emulate refillable cartridges using an integrated circuit called the SMARTEK chip. The SMARTEK chip contained a communications interface, microprocessor, and firmware program that reproduced the authentication sequence used by the Lexmark's printers. The court held that the defendant circumvented an access control measure because the firmware in the defendant's cartridges performed a "secret handshake" (authentication) process to gain access to Lexmark's copyrighted Toner Loading Programs and Printer Engine Programs.[82] The court explained that Lexmark's authentication sequence effectively "controls access" to the Toner Loading Programs and the Printer Engine Program because

[81] Lexmark Int'l, Inc. v. Static Control Components, Inc., 253 F. Supp. 2d 943 (E.D. Ky. 2003)

[82] *Id.*, at 967-68.

it controls the consumer's ability to make use of these programs.[83] In making this determination, the court cited both the *Gamemasters* and *Streambox* cases described above. The court stated that "[t[he access control measure upheld by the *Gamemasters* court is, as a technical matter, virtually identical to, and as a legal matter, indistinguishable from, the access control measure employed by Lexmark in the instant case."[84] "If the printer cannot verify that the cartridge is, in fact, such a product, the Printer Engine Program will not operate and will not [execute] the Toner Loading Program. [The Static Control Components] SMARTEK microchips, like the "Game Enhancer" device in *Gamemasters,* circumvents the access control measure on the Lexmark printer 'that ensures the [printer] operates only when encrypted data is read from an authorized [toner cartridge].'"[85] Thus, just as access control measures in *Gamemasters*

The distinction between access and copy control is likely to become even less clear with the growth of Digital Rights Management (DRM) frameworks. Digital rights management is the infrastructure to support secure promotion, sale, and delivery of digital content.[86] The infrastructure consists of cooperating autonomous components that perform the following main functions:

---

[83] *Id*. At 968, citing *GameMasters,* 87 F. Supp. 2d at 987. (Sony's PlayStation console contained a technological measure that controlled a consumer's ability to make use of copyrighted computer programs.)

[84] *Id*. at 970.

[85] *Id*.

[86] Barbara Fox, *DRM Technology Overview,* (Feb. 27, 2003)(presentation at Berkeley Conference on Law and Technology of DRM Systems) *at* http://www.law.berkeley.edu/institutes/bclt/drm/slides/bf_slides_files/frame.htm (last visited March, 2004).

1. Authentication of the content (video, music, software, game, etc.), user, and the system (computer, game system, video device, etc.) being used to view, play, or execute the content
2. The capability to encrypt copyrighted digital content and to decrypt such content for an authenticated licensed user on an authenticated authorized system
3. A means by which the content supplier can specify the rights the supplier grants to a user
4. The capability to define and enforce policies on delegation of licensing granting powers and transfer of licensed rights

The criteria that courts will use to classify these functions as either access control, copy control, or both are not readily apparent.

Although there is often little if any factual difference between access and copy control technical measures, the legal distinction can be quite important. Under the DMCA, an individual *is not prohibited* from circumventing a *copy control technical measure* (the U.S. Copyright Office has explained this exemption to allow for fair use[87]) but *is prohibited* from circumventing an *access control measure.* The difficulty that courts have in distinguishing between access and copy control is troubling because the classification can often affect the outcome. For example, because CSS was characterized as an access control measure, the *Reimerdes* court rejected defendants' argument that using DeCSS to decrypt a disk was allowable under the exemption in section 1201(b).[88]

---

[87] The Digital Millennium Copyright Act of 1998, U.S. Copyright Office Summary (Dec. 1998), *available at* http://www.copyright.gov/legislation/dmca.pdf (last visited March 6, 2004).

[88] *Reimerdes*, 111 F.Supp.2d at 316, n. 133. It should be noted that this was *one* of the arguments that the court rejected. As noted earlier, the court rejected other arguments by the defendant when it issued the injunction.

D. Difficulty Determining the Primary Purpose of a Software Package

If software were structured in a manner that its runtime components were written either purely for the purposes of copy/access protection or purely for the purposes of functionality, then the law would be clear. However, in software, it is possible to incorporate *both* protection *and* functionality into the same components. Thus, persons trying to determine whether reverse engineering is permissible face uncertainty.

The anti-trafficking provisions of sections 1201(a)(2) and 1201(b)(1) that subject a defendant to liability require a court to determine whether a device or technology is "*primarily* designed or produced for the purpose of circumventing a technological measure", and has "limited commercially significant purpose or use other than to circumvent such a technological measure."

Whether software containing circumvention measures is designed "primarily" for the purposes of circumvention is difficult to determine. Unlike defendants using pure hardware devices, defendants using software cannot demonstrate the cost of materials, manufacturing, and distribution, and show the overall cost and value of the circumvention technology relative to that of the total product. When the technology at issue is composed entirely of or contains a significant amount of software, courts have held that the product *is* primarily designed or produced for the purposes of intervention *even if most of the functionality of the software has nothing at all to do with circumvention.*

In *Realnetworks, Inc. v. Streambox, Inc.,* 2000 U.S. Dist. LEXIS 1889 the court ruled for the plaintiff and granted an injunction against distributing the defendant's software product, the Streambox VCR "because *at least a part* of the Streambox VCR is primarily, if not exclusively, designed to circumvent the access control and copy

protection measures that RealNetworks affords to copyright owners."[89] . The court stated that "the [Streambox] VCR that circumvents the Secret Handshake so as to avoid the Copy Switch has no significant commercial purpose other than to enable users to access and record protected content."[90] In so doing, the court weighed the "secret handshake" (which is little more than supplying a valid password) and copy switch override (which is removal of functionality to check for copy permission), to be legally more significant than all other Streambox VCR software functions. Such functions included managing multimedia file downloads from the server, interpreting the multimedia file content in multiple formats, interfacing with the sound generation and video display hardware on the user's computer, and managing the display for the user.

Similarly, in *Sony Computer Entertainment America, Inc. v. Gamemasters,* the court granted the plaintiff's preliminary injunction, finding a likelihood that it would prevail because the defendant's game enhancement software appeared to primarily function as a circumvention measure. The court's conclusion disregarded the defendant's assertions that the purpose of the offending software was to enable users to alter the parameters of games (e.g., the amount of ammunition or "lives" available to a character in an adventure game) thereby altering or, from the perspective of the user, "enhancing" the game (hence the product's name).

In *Chamberlain Group v. Skylink, Inc.*,[91] the plaintiff alleged that the defendant's remote garage door opener (GDO) transmitter violated the access control provision of the

---

[89] *Streambox*, 2000 U.S. Dist. LEXIS at 20-21(emphasis added).

[90] *Id.* at 21.

[91] Chamberlain Group v. Skylink, Inc., 292 F. Supp. 2d 1023(N.D. Ill. , 2003). Available at http://www.ipjustice.org/skylink/082903_ORDER.pdf

DMCA because, inter alia, it emulated a "rolling code" scheme in which a part of the transmission sequence was changed each time the transmitter was activated. The defendant argued that the GDO transmitter in question was a "universal" model and therefore emulated multiple transmitters, most of which did not use the rolling code scheme. The found held that for the purposes of a summary judgment motion, the product was designed primarily for circumvention. The court stated:

> Skylink [defendant and non-moving party] has provided evidence that the Model 39 transmitter [the offending GDO] *serves purposes other than circumventing.* It is now Chamberlain's [plaintiff and moving party] burden to establish that those other purposes do not prevent this court from finding the Model 39 in violation of the DMCA. *For purposes of this decision* [on the plaintiff's motion for summary judgment]*, the court will assume that Chamberlain has done so.* Like the Plaintiff in *RealNetworks,* Chamberlain has demonstrated that the Model 39 transmitter has one particular setting that serves only one function: to operate the Chamberlain rolling code GDO. Accordingly, the fact that the Model 39 transmitter serves more than one purpose may not be sufficient to deny summary judgment in this matter.[92]

The court denied the motion for summary judgment on two other grounds: (a) the defendant had raised a question of fact as to whether the code in question was actually copyrighted, and (b) the plaintiff did not explicitly prohibit purchasers from acquiring aftermarket transmitters from other suppliers, and that homeowners have a legitimate expectation that "…universal transmitters being marketed and sold [would] allow homeowners an alternative means to access any brand of GDO."[93] Had the plaintiff's product been an entertainment or game device, then the judge's view of "consumer expectations" might have resulted in the *Streambox* or *Gamemasters* outcome.

---

[92] *Id*. at 44 (emphasis added).

[93] *Id*. at 50-51.

The trend of these decisions would tend suggests that it would be imprudent for a person to reverse engineer a software product with *any* access or copy protection, and conversely, that from the plaintiff's side, the best barrier to entry that could be erected against emulators would be to include *any* copy protection in the code.

The consequences of a continuation of this trend will result in a reduction in competition.[94] By encrypting the data files of its products, any product vendor could effectively eliminate competition in an aftermarket. Thus, for example, an automobile manufacturer could prohibit the use of "unauthorized" tires (made by companies other than those with which it had agreements) by virtue of an embedded processor with firmware contained on the tire that exchanged an encryption key with the automobile chassis. Indeed, the use of encryption could eviscerate the entire "useful article" doctrine that attempts to distinguish the utilitarian aspects of an article from its design and appearance.[95]

Nor would this outcome be limited to hardware products that contain firmware. One could imagine software developers choosing to encrypt their data files thereby prohibiting competitors from creating compatible products. Thus, the producers of Word Perfect™ might have prevented Microsoft Word™ from entering the legal market through file encryption thereby prohibiting file compatibility. It is somewhat ironic that those arguing for this position were probably producing their documents on personal

---

[94] *See* Ronald Katz and Adan Safer, supra note 2..

[95] *See, e.g.,* Brandir Int'l, Inc. v. Cascade Pacific Lumber Co., 834 F.2d 1142 (2d Cir. 1987) (bicycle rack is not copyrightable because in its final form it is essentially a product of industrial design). *See also* H.R. REP. NO. 94-1476, 94th Cong. (2d Sess. 1976) 47-55 (declaration that pictorial graphic, and sculptural works includes works of artistic craftsmanship insofar as their form but not their mechanical or utilitarian aspects are concerned).

computers with firmware reverse engineered from the original IBM PC and whose distribution could be prohibited if courts adapt their position.

IV. Recommendations

The difficulties described in the previous section can be addressed through following changes in the law or in interpretation by the courts:

1. *Specify that only software components dedicated to copy or access control are entitled to anti-circumvention protection and require that code be clearly labeled and identified.* By restricting section 1201 protection to code that is developed exclusively to protect the rights of content owners, nearly all of the uncertainty associated with reverse engineering can be eliminated. This restriction will enable the congressional intent in passing the DMCA to be realized while at the same time mitigating the chilling and economic uncertainty involved in the development of consumer products.
2. *Allow an affirmative defense of misuse for firmware incorporated into objects that are "useful articles"*[96] *previously did not qualify for copyright protection.* Copyright protection was limited to "works of authorship" and not functional or utilitarian objects such as laser printer toner cartridges or transmitters for garage door openers. Manufacturers should not be able to create a monopoly simply by inserting a chip with firmware implementing

[96] *See* 17 U.S.C. 101 ("A 'useful article' is an article having an intrinsic utilitarian function that is not merely to portray the appearance of the article or to convey information").

a simple handshake protocol into a standard consumer product with the intention of creating a legal barrier to potential competitors.

3. *Explicitly allow for free discussion of circumvention prohibitions that are not reduced to code.* As of the time of the writing of this Article, no court has ruled on the question of whether *mere discussion* of copy protection or access control circumvention methods constitutes a violation of the DMCA. However, threatening letters written by vendors such as those cited in Part III.A.1 have largely served this function. Few computer scientists, who have many research options open to them, would choose to place at risk their time and assets to test the law. A legal situation in which vendors can make such threats and effectively silence a vigorous and important area of research is not only inherently unjust, it places society at risk because only through public discussion and analysis have effective security algorithms been developed. If an explicit letter threatening prosecution for alleged DMCA violations is deemed to be unfair to copyright holders, then a cause of action should be developed for frivolous use of such threats.

These changes will mitigate the difficulties in section 1201 of the DMCA by removing the uncertainty associated with engaging in reverse engineering, emulation, and legitimate computer security research. They are broader in scope but not exclusive of

other proposed congressional changes such as the BALANCE Act of 2003[97] or the Digital Media Consumers' Rights Act[98] which allow relaxation of anti-circumvention provisions primarily for the purposes of allowing consumers to have greater freedom in making backup copies.

The goals of the DMCA and of the anti-circumvention measures--to encourage distribution of literary and artistic works over the Internet–are important and valid. However, the means of achieving these goals should not unnecessarily restrict the activities of the technology community, which remains one of the most robust and vigorous forces for change in our society.

---

[97] *Section By Section Analysis of Rep. Lofgren's Balance Act of 2003, at* http://www.house.gov/lofgren/news/2002/secbysecbalance.htm (last visited March 6, 2004).

[98] *Digital Media Consumer's Rights Act, available at* http://www.house.gov/boucher/docs/dmcrahandout.htm (last visited March 6, 2004).