UNITED STATES DISTRICT COURT
SOUTHERN DISTRICT OF NEW YORK

- x

UNIVERSAL CITY STUDIOS, INC, et al.,

Plaintiffs,

-against- 00 Civ. 0277 (LAK)

SHAWN C. REIMERDES, et al.,

Defendants.

- x

OPINION

Appearances:

Leon P. Gold
Jon A. Baumgarten
Charles S. Sims
Scott P. Cooper
William M. Hart
Michael M. Mervis
Carla M. Miller
PROSKAUER ROSE LLP
Attorneys for Plaintiffs

Martin Garbus
George E. Singleton
David Y. Atlas
Edward Hernstadt
FRANKFURT, GARBUS, KLEIN & SELZ, P.C.
Attorneys for Defendants

Contents

I. The Genesis of the Controversy 3

A. The Vocabulary of this Case 4

1. Computers and Operating Systems 4

2. Computer Code 5

3. The Internet and the World Wide Web 7

4. Portable Storage Media 9

5. The Technology Here at Issue 10

B. Parties 11

C. The Development of DVD and CSS 13

D. The Appearance of DeCSS 17

E. The Distribution of DeCSS 19

F. The Preliminary Injunction and Defendants' Response 20

G. Effects on Plaintiffs 22

II. The Digital Millennium Copyright Act 28

A. Background and Structure of the Statute 28

B. Posting of DeCSS 30

1. Violation of Anti-Trafficking Provision 30

a. Section 1201(a)(2)(A) 32

(1) CSS Effectively Controls Access to Copyrighted Works 32

(2) DeCSS Was Designed Primarily to Circumvent CSS . . . 34

b. Section 1201(a)(2)(B) 34

c. The Linux Argument 35

2. Statutory Exceptions 36

a. Reverse engineering 36

b. Encryption research 38

c. Security testing 40

d. Fair use 40

C. Linking to Sites Offering DeCSS 46

III. The First Amendment 49

A. Computer Code and the First Amendment 50

B. The Constitutionality of the DMCA's Anti-Trafficking Provision 52

1. Defendants' Alleged Right to Disseminate DeCSS 52

2. Prior Restraint 64

3. Overbreadth 69

4. Vagueness 75

C. Linking 76

IV. Relief 81

A. Injury to Plaintiffs 81

B. Permanent Injunction and Declaratory Relief 83

V. Miscellaneous Contentions 88

VI. Conclusion 89

LEWIS A. KAPLAN, *District Judge.*

Plaintiffs, eight major United States motion picture studios, distribute many of their copyrighted motion pictures for home use on digital versatile disks ("DVDs"), which contain copies of the motion pictures in digital form. They protect those motion pictures from copying by using an encryption system called CSS. CSS-protected motion pictures on DVDs may be viewed only on players and computer drives equipped with licensed technology that permits the devices to decrypt and play—but not to copy—the films.

Late last year, computer hackers devised a computer program called DeCSS that circumvents the CSS protection system and allows CSS-protected motion pictures to be copied and played on devices that lack the licensed decryption technology. Defendants quickly posted DeCSS on their Internet web site, thus making it readily available to much of the world. Plaintiffs promptly brought this action under the Digital Millennium Copyright Act (the "DMCA")[1] to enjoin defendants from posting DeCSS and to prevent them from electronically "linking" their site to others that post DeCSS. Defendants responded with what they termed "electronic civil disobedience"—increasing their efforts to link their web site to a large number of others that continue to make DeCSS available.

Defendants contend that their actions do not violate the DMCA and, in any case, that the DMCA, as applied to computer programs, or code, violates the First Amendment.[2] This is the

---

[1] 17 U.S.C. § 1201 *et seq.*

[2] Shortly after the commencement of the action, the Court granted plaintiffs' motion for a preliminary injunction barring defendants from posting DeCSS. *Universal City Studios, Inc. v. Reimerdes*, 82 F. Supp.2d 211 (S.D.N.Y. 2000). Subsequent motions to expand the preliminary injunction to linking and to vacate it were consolidated with the trial on the merits. This opinion reflects the Court's findings of fact, conclusions of law and decision on the merits.

The Court notes the receipt of a number of *amicus* submissions. Although many were filed

Court's decision after trial, and the decision may be summarized in a nutshell.

Defendants argue first that the DMCA should not be construed to reach their conduct, principally because the DMCA, so applied, could prevent those who wish to gain access to technologically protected copyrighted works in order to make fair—that is, non-infringing—use of them from doing so. They argue that those who would make fair use of technologically protected copyrighted works need means, such as DeCSS, of circumventing access control measures not for piracy, but to make lawful use of those works.

Technological access control measures have the capacity to prevent fair uses of copyrighted works as well as foul. Hence, there is a potential tension between the use of such access control measures and fair use. Defendants are not the first to recognize that possibility. As the DMCA made its way through the legislative process, Congress was preoccupied with precisely this issue. Proponents of strong restrictions on circumvention of access control measures argued that they were essential if copyright holders were to make their works available in digital form because digital works otherwise could be pirated too easily. Opponents contended that strong anti-circumvention measures would extend the copyright monopoly inappropriately and prevent many fair uses of copyrighted material.

Congress struck a balance. The compromise it reached, depending upon future technological and commercial developments, may or may not prove ideal.[3] But the solution it enacted is clear. The potential tension to which defendants point does not absolve them of liability under the

---

by defendants' counsel on behalf of certain *amici*, and therefore were of debatable objectivity, the *amicus* submissions considered as a group were helpful.

[3] David Nimmer, *A Riff on Fair Use in the Digital Millennium Copyright Act*, 148 U. PA. L. REV. 673, 739-41 (2000) (hereinafter *A Riff on Fair Use*).

statute. There is no serious question that defendants' posting of DeCSS violates the DMCA.

Defendants' constitutional argument ultimately rests on two propositions—that computer code, regardless of its function, is "speech" entitled to maximum constitutional protection and that computer code therefore essentially is exempt from regulation by government. But their argument is baseless.

Computer code is expressive. To that extent, it is a matter of First Amendment concern. But computer code is not purely expressive any more than the assassination of a political figure is purely a political statement. Code causes computers to perform desired functions. Its expressive element no more immunizes its functional aspects from regulation than the expressive motives of an assassin immunize the assassin's action.

In an era in which the transmission of computer viruses—which, like DeCSS, are simply computer code and thus to some degree expressive—can disable systems upon which the nation depends and in which other computer code also is capable of inflicting other harm, society must be able to regulate the use and dissemination of code in appropriate circumstances. The Constitution, after all, is a framework for building a just and democratic society. It is not a suicide pact.

I. The Genesis of the Controversy

As this case involves computers and technology with which many are unfamiliar, it is useful to begin by defining some of the vocabulary.

A. The Vocabulary of this Case

1. Computers and Operating Systems

A computer is "a digital information processing device . . . . consist[ing] of central processing components . . . and mass data storage . . . . certain peripheral input/output devices . . . , and an operating system." Personal computers ("PCs") are computers designed for use by one person at a time. "[M]ore powerful, more expensive computer systems known as 'servers' . . . are designed to provide data, services, and functionality through a digital network to multiple users."[4]

An operating system is "a software program that controls the allocation and use of computer resources (such as central processing unit time, main memory space, disk space, and input/output channels). The operating system also supports the functions of software programs, called 'applications,' that perform specific user-oriented tasks . . . . Because it supports applications while interacting more closely with the PC system's hardware, the operating system is said to serve as a 'platform.'"[5]

Microsoft Windows ("Windows") is an operating system released by Microsoft Corp. It is the most widely used operating system for PCs in the United States, and its versions include Windows 95, Windows 98, Windows NT and Windows 2000.

Linux, which was and continues to be developed through the open source model of

---

[4] *United States v. Microsoft Corp.*, 84 F. Supp.2d 9, 13 (D. D.C. 1999). The quotations are from a finding of fact in the *Microsoft* case of which the Court, after notice to and without objection by the parties, takes judicial notice. Tr. at 1121. Subsequent references to *Microsoft* findings reflect similar instances of judicial notice without objection.

[5] *United States v. Microsoft Corp.*, 84 F. Supp.2d at 13.

software development,[6] also is an operating system.[7] It can be run on a PC as an alternative to Windows, although the extent to which it is so used is limited.[8] Linux is more widely used on servers.[9]

2. Computer Code

"[C]omputers come down to one basic premise: They operate with a series of on and off switches, using two digits in the binary (base 2) number system—0 (for off) and 1 (for on)."[10] All data and instructions input to or contained in computers therefore must be reduced the numerals 1 and 0.[11]

"The smallest unit of memory in a computer," a bit, "is a switch with a value of 0 (off)

---

6 Open source is a software development model by which the source code to a computer program is made available publicly under a license that gives users the right to modify and redistribute the program. The program develops through this process of modification and redistribution and through a process by which users download sections of code from a web site, modify that code, upload it to the same web site, and merge the modified sections into the original code. Trial transcript ("Tr.") (Craig) at 1008.

7 Tr. (Pavlovich) at 936.

8 Tr. (DiBona) at 994-95.

9 *Id.*

10 THE NEW YORK PUBLIC LIBRARY, SCIENCE DESK REFERENCE 496 (1995) (hereinafter SCIENCE DESK REFERENCE); *see also* Tr. (Felten) at 758-59; Hon. Shira A. Scheindlin & Jeffrey Rabkin, *Electronic Discovery in Federal Civil Litigation: Is Rule 34 Up to the Task?* 34 B. C. L. REV. 327, 333-35 (2000).

11 Tr. (Felten) at 759; Scheindlin & Rabkin, 34 B. C. L. REV. at 333-35.

or 1 (on)."[12] A group of eight bits is called a byte and represents a character—a letter or an integer.[13] A kilobyte ("K") is 1024 bytes, a megabyte ("MB") 1024 kilobytes, and a gigabyte ("GB") 1024 megabytes.[14]

Some highly skilled human beings can reduce data and instructions to strings of 1's and 0's and thus program computers to perform complex tasks by inputting commands and data in that form.[15] But it would be inconvenient, inefficient and, for most people, probably impossible to do so. In consequence, computer science has developed programming languages. These languages, like other written languages, employ symbols and syntax to convey meaning. The text of programs written in these languages is referred to as source code.[16] And whether directly or through the medium of another program,[17] the sets of instructions written in programming languages—the source code—ultimately are translated into machine "readable" strings of 1's and 0's, known in the computer

---

12 SCIENCE DESK REFERENCE, at 501.

13 *Id.*

14 *Id.*

15 *See* Tr. (Felten) at 759-60.

16 The Court's findings with respect to the definitions of source code and object code are taken from the trial testimony of Robert Schumann, Tr. at 258, and Drs. Edward Felten, Tr. at 738-39, 757-63, David S. Touretzky, Tr. at 1065-91, and Andrew Appel, Tr. at 1096, and the deposition testimony of Dr. Harold Abelson, Ex. AZO at 34-37, 45-49. *See also* Ex. BBE.

17 Frequently, programs written in such languages must be transformed or translated into machine readable form by other programs known as compilers.

world as object code, which typically are executable by the computer.[18]

The distinction between source and object code is not as crystal clear as first appears. Depending upon the programming language, source code may contain many 1's and 0's and look a lot like object code or may contain many instructions derived from spoken human language. Programming languages the source code for which approaches object code are referred to as low level source code while those that are more similar to spoken language are referred to as high level source code.

All code is human readable. As source code is closer to human language than is object code, it tends to be comprehended more easily by humans than object code.

3. The Internet and the World Wide Web

The Internet is "a global electronic network, consisting of smaller, interconnected networks, which allows millions of computers to exchange information over telephone wires, dedicated data cables, and wireless links. The Internet links PCs by means of servers, which run specialized operating systems and applications designed for servicing a network environment."[19]

Internet Relay Chat ("IRC") is a system that enables individuals connected to the

---

18 This to some degree is an oversimplification. Object code often is directly executable by the computer into which it is entered. It sometimes contains instructions, however, that are readable only by computers containing a particular processor, such as a Pentium processor, or a specific operating system such as Microsoft Windows. In such instances, a computer lacking the specific processor or operating system can execute the object code only if it has an emulator program that simulates the necessary processor or operating system or if the code first is run through a translator program that converts it into object code readable by that computer. Ex. BBE.

19 *United States v. Microsoft Corp.*, 84 F. Supp.2d at 13.

Internet to participate in live typed discussions.[20] Participation in an IRC discussion requires an IRC software program, which sends messages via the Internet to the IRC server, which in turn broadcasts the messages to all participants. The IRC system is capable of supporting many separate discussions at once.

The World Wide Web (the "Web") is "a massive collection of digital information resources stored on servers throughout the Internet. These resources are typically provided in the form of hypertext documents, commonly referred to as 'Web pages,' that may incorporate any combination of text, graphics, audio and video content, software programs, and other data. A user of a computer connected to the Internet can publish a page on the Web simply by copying it into a specially designated, publicly accessible directory on a Web server. Some Web resources are in the form of applications that provide functionality through a user's PC system but actually execute on a server."[21]

A web site is "a collection of Web pages [published on the Web by an individual or organization] . . . . Most Web pages are in the form of 'hypertext'; that is, they contain annotated references, or 'hyperlinks,' to other Web pages. Hyperlinks can be used as cross-references within a single document, between documents on the same site, or between documents on different sites."[22]

A home page is "one page on each Web site . . . [that typically serves as] the first access point to the site. The home page is usually a hypertext document that presents an overview

---

[20] Tr. (Shamos) at 67-68.

[21] *United States v. Microsoft Corp.*, 84 F. Supp.2d at 13.

[22] *Id.* at 14.

of the site and hyperlinks to the other pages comprising the site."[23]

A Web client is "software that, when running on a computer connected to the Internet, sends information to and receives information from Web servers throughout the Internet. Web clients and servers transfer data using a standard known as the Hypertext Transfer Protocol ('HTTP'). A 'Web browser' is a type of Web client that enables a user to select, retrieve, and perceive resources on the Web. In particular, Web browsers provide a way for a user to view hypertext documents and follow the hyperlinks that connect them, typically by moving the cursor over a link and depressing the mouse button."[24]

4. Portable Storage Media

Digital files may be stored on several different kinds of storage media, some of which are readily transportable. Perhaps the most familiar of these are so called floppy disks or "floppies," which now are 3 ½ inch magnetic disks upon which digital files may be recorded.[25] For present purposes, however, we are concerned principally with two more recent developments, CD-ROMs and digital versatile disks, or DVDs.

A CD-ROM is a five-inch wide optical disk capable of storing approximately 650 MB

---

23 *Id.*

24 *Id.*

25 Not too many years ago, the most common transportable storage media were 5 ¼ inch flexible magnetic disks. Their flexibility led to their being referred to as "floppies." They have been replaced almost entirely with today's 3 ½ inch disks, which are enclosed in hard plastic housings and which therefore are not flexible or "floppy." The earlier name, however, has stuck.

of data. To read the data on a CD-ROM, a computer must have a CD-ROM drive.

DVDs are five-inch wide disks capable of storing more than 4.7 GB of data. In the application relevant here, they are used to hold full-length motion pictures in digital form. They are the latest technology for private home viewing of recorded motion pictures and result in drastically improved audio and visual clarity and quality of motion pictures shown on televisions or computer screens.[26]

5. The Technology Here at Issue

CSS, or Content Scramble System, is an access control and copy prevention system for DVDs developed by the motion picture companies, including plaintiffs.[27] It is an encryption-based system that requires the use of appropriately configured hardware such as a DVD player or a computer DVD drive to decrypt, unscramble and play back, but not copy, motion pictures on DVDs.[28] The technology necessary to configure DVD players and drives to play CSS-protected DVDs[29] has been licensed to hundreds of manufacturers in the United States and around the world.

DeCSS is a software utility, or computer program, that enables users to break the CSS copy protection system and hence to view DVDs on unlicenced players and make digital copies of

---

[26] Tr. (King) at 403-04.

[27] Tr. (Shamos) at 24.

[28] *Id.* at 24-25.

[29] Such devices are referred to subsequently as compliant.

DVD movies.[30] The quality of motion pictures decrypted by DeCSS is virtually identical to that of encrypted movies on DVD.[31]

DivX is a compression program available for download over the Internet.[32] It compresses video files in order to minimize required storage space, often to facilitate transfer over the Internet or other networks.[33]

B. Parties

Plaintiffs are eight major motion picture studios. Each is in the business of producing and distributing copyrighted material including motion pictures. Each distributes, either directly or through affiliates, copyrighted motion pictures on DVDs.[34] Plaintiffs produce and distribute a large majority of the motion pictures on DVDs on the market today.[35]

Defendant Eric Corley is viewed as a leader of the computer hacker community and goes by the name Emmanuel Goldstein, after the leader of the underground in George Orwell's

---

30 Tr. (Shamos) at 25.

31 Tr. (Schumann) at 273.

32 Tr. (Ramadge) at 911.

33 *Id.* at 911-12.

34 Ex. 2.1-2.34; 3.1-3.34.

35 Tr. (King) at 404.

classic, *1984*.[36] He and his company, defendant 2600 Enterprises, Inc., together publish a magazine called *2600: The Hacker Quarterly*, which Corley founded in 1984,[37] and which is something of a bible to the hacker community.[38] The name "2600" was derived from the fact that hackers in the 1960's found that the transmission of a 2600 hertz tone over a long distance trunk connection gained access to "operator mode" and allowed the user to explore aspects of the telephone system that were not otherwise accessible.[39] Mr. Corley chose the name because he regarded it as a "mystical thing,"[40] commemorating something that he evidently admired. Not surprisingly, *2600: The Hacker Quarterly* has included articles on such topics as how to steal an Internet domain name,[41] access other people's e-mail,[42] intercept cellular phone calls,[43] and break into the computer systems at Costco stores[44] and

---

36 Tr. (Corley) at 787, 827.

37 Tr. (Corley) at 777, 790, 795; Ex. 1.1, 1.2, 1.3, 1.4, 1.5, 1.6, 1.7, 1.8, 1.11, 1.12, 1.13, 1.14, 1.15, 1.16; 79 (Corley Dec.) ¶ 1.

38 *See* Tr. (Corley) at 781.

39 Tr. (Corley) 786-87.

40 *Id.* at 787.

41 Ex. 1.2 (Redomega Crim, *How Domains Are Stolen*, 2600: THE HACKER QUARTERLY, Summer 2000, at 43).

42 Ex. 1.16 (Schlork, *Snooping via MS-Mail*, 2600: THE HACKER QUARTERLY, Winter 1996-97, at 28).

43 Ex. 1.14 (Thomas Icom, *Cellular Interception Techniques*, 2600: THE HACKER QUARTERLY, Spring 1995, at 23).

44 Ex. 1.12 (nux, *Fun at Costco*, 2600: THE HACKER QUARTERLY, Summer 1999, at 12).

Federal Express.[45] One issue contains a guide to the federal criminal justice system for readers charged with computer hacking.[46] In addition, defendants operate a web site located at <http://www.2600.com> ("2600.com"), which is managed primarily by Mr. Corley and has been in existence since 1995.[47]

Prior to January 2000, when this action was commenced, defendants posted the source and object code for DeCSS on the 2600.com web site, from which they could be downloaded easily.[48] At that time, 2600.com contained also a list of links to other web sites purporting to post DeCSS.[49]

C. The Development of DVD and CSS

The major motion picture studios typically distribute films in a sequence of so-called windows, each window referring to a separate channel of distribution and thus to a separate source of revenue. The first window generally is theatrical release, distribution, and exhibition.

---

45 Ex. 1.19 (PhranSys Drak3, *Hacking FedEx,* 2600: THE HACKER QUARTERLY, Autumn 1997, at 14).

46 Ex. 1.19 (Agent Steal, *Busted! A Complete Guide to Getting Caught*, 2600: THE HACKER QUARTERLY, Autumn 1997, at 6).

47 Tr. (Corley) at 790; Ex. 52-54, 64, 79 (Corley Dec.) ¶ 20; 97.

Interestingly, defendants' copyright both their magazine and the material on their web site to prevent others from copying their works. Tr. (Corley) at 832; Ex. 96 (Corley Dep.) at 23-24.

48 Tr. (Corley) at 791; Ex. 28.

49 Tr. (Corley) at 791, 829, 848; Ex. 28.

Subsequently, films are distributed to airlines and hotels, then to the home market, then to pay television, cable and, eventually, free television broadcast. The home market is important to plaintiffs, as it represents a significant source of revenue.[50]

Motion pictures first were, and still are, distributed to the home market in the form of video cassette tapes. In the early 1990's, however, the major movie studios began to explore distribution to the home market in digital format, which offered substantially higher audio and visual quality and greater longevity than video cassette tapes.[51] This technology, which in 1995 became what is known today as DVD,[52] brought with it a new problem—increased risk of piracy by virtue of the fact that digital files, unlike the material on video cassettes, can be copied without degradation from generation to generation.[53] In consequence, the movie studios became concerned as the product neared market with the threat of DVD piracy.[54]

Discussions among the studios with the goal of organizing a unified response to the piracy threat began in earnest in late 1995 or early 1996.[55] They eventually came to include representatives of the consumer electronics and computer industries, as well as interested members

---

50 Tr. (King) at 402.

51 *Id.* at 404, 468.

52 *Id.* at 408, 468, 470.

53 *Id.* at 404-05.

54 *Id.* at 404-05, 468-70.

55 *Id.* at 406.

of the public,[56] and focused on both legislative proposals and technological solutions.[57] In 1996, Matsushita Electric Industrial Co. ("MEI") and Toshiba Corp., presented—and the studios adopted—CSS.[58]

CSS involves encrypting, according to an encryption algorithm,[59] the digital sound and graphics files on a DVD that together constitute a motion picture. A CSS-protected DVD can be decrypted by an appropriate decryption algorithm that employs a series of keys stored on the DVD and the DVD player. In consequence, only players and drives containing the appropriate keys are able to decrypt DVD files and thereby play movies stored on DVDs.

As the motion picture companies did not themselves develop CSS and, in any case, are not in the business of making DVD players and drives, the technology for making compliant devices, i.e., devices with CSS keys, had to be licensed to consumer electronics manufacturers.[60] In order to ensure that the decryption technology did not become generally available and that compliant devices could not be used to copy as well as merely to play CSS-protected movies, the technology

---

56 *Id.* at 405-06, 471, 476-78.

57 *Id.* at 405, 470-71, 479.

58 *Id.* at 406-07, 502-04.

59 An algorithm is a recipe that contains instructions for completing a task. It can be expressed in any language, from natural spoken language to computer programming language. Ex. AZO (Abelson Dep.) at 9-10.

60 The licensing function initially was performed by MEI and Toshiba. Subsequently, MEI and Toshiba granted a royalty free license to the DVD Copy Control Association ("DVD CCA"), which now handles the licensing function. Tr. (King) at 485-86, 510; Ex. XXY (Attaway Dep.) at 31. The motion picture companies themselves license CSS from the DVD CCA. Ex. XYY (Attaway Dep.) at 31-32.

is licensed subject to strict security requirements.[61] Moreover, manufacturers may not, consistent with their licenses, make equipment that would supply digital output that could be used in copying protected DVDs.[62] Licenses to manufacture compliant devices are granted on a royalty-free basis subject only to an administrative fee.[63] At the time of trial, licenses had been issued to numerous hardware and software manufacturers, including two companies that plan to release DVD players for computers running the Linux operating system.[64]

With CSS in place, the studios introduced DVDs on the consumer market in early 1997.[65] All or most of the motion pictures released on DVD were, and continue to be, encrypted with CSS technology.[66] Over 4,000 motion pictures now have been released in DVD format in the United States, and movies are being issued on DVD at the rate of over 40 new titles per month in addition to rereleases of classic films. Currently, more than five million households in the United

---

61 *See, e.g.,* Ex. AHV §§ 5, 6.2.

62 Tr. (King) at 450-51, 492-93; Ex. XXY (Attaway Dep.) at 61-62; Ex. AHV.

63 The administrative fee is one million yen, now about $9,200, for each "membership category" selected by the licensee. Twelve membership categories are available, and one or more are selected by a licensee depending on the use which the licensee intends to make of the licensed technology. The membership categories are: content provider, authoring studio, DVD disc replicator, DVD player manufacturer, DVD-ROM drive manufacturer, DVD decoder manufacturer, descramble module manufacturer, authentication chip manufacturer for DVD-ROM drive, authenticator manufacturer for DVD decoder, integrated product manufacturer, and reseller. Ex. AJB, AIZ, AOV, AOU, AOQ.

64 Tr. (King) at 437-38; *see also* Tr. (Pavolvich) at 961; Ex. BD.

65 Tr. (King) at 408-09.

66 *Id.* at 409.

States own DVD players,[67] and players are projected to be in ten percent of United States homes by the end of 2000.[68]

DVDs have proven not only popular, but lucrative for the studios. Revenue from their sale and rental currently accounts for a substantial percentage of the movie studios' revenue from the home video market.[69] Revenue from the home market, in turn, makes up a large percentage of the studios' total distribution revenue.[70]

D. The Appearance of DeCSS

In late September 1999, Jon Johansen, a Norwegian subject then fifteen years of age, and two individuals he "met" under pseudonyms over the Internet, reverse engineered a licensed DVD player and discovered the CSS encryption algorithm and keys.[71] They used this information to create DeCSS, a program capable of decrypting or "ripping" encrypted DVDs, thereby allowing playback on non-compliant computers as well as the copying of decrypted files to computer hard

---

67 *Id.* at 417-18.

68 *Id.* at 442.

69 Revenue from the distribution of DVDs makes up approximately 35 percent of Warner Brothers' total worldwide revenue from movie distribution in the home video market. *Id.* at 403.

70 Distribution in the home video market accounts for approximately 40 percent of Warner Brothers' total income from movie distribution. *Id.*

71 Tr. (Johansen) at 619-22, 633, 639.

drives.[72] Mr. Johansen then posted the executable code on his personal Internet web site and informed members of an Internet mailing list that he had done so.[73] Neither Mr. Johansen nor his collaborators obtained a license from the DVD CCA.[74]

Although Mr. Johansen testified at trial that he created DeCSS in order to make a DVD player that would operate on a computer running the Linux operating system,[75] DeCSS is a Windows executable file; that is, it can be executed only on computers running the Windows operating system.[76] Mr. Johansen explained the fact that he created a Windows rather than a Linux program by asserting that Linux, at the time he created DeCSS, did not support the file system used on DVDs.[77] Hence, it was necessary, he said, to decrypt the DVD on a Windows computer in order subsequently to play the decrypted files on a Linux machine.[78] Assuming that to be true,[79] however,

---

72 *Id.* at 619-21, 634; (Schumann) at 246-48. Mr. Johansen testified that the "De" in DeCSS stands for "decrypt." Tr. (Johansen) at 628.

73 Tr. (Johansen) at 622-23, 638; Ex. 9 at SCH-000846. Mr. Johansen did not post the source code on his Web site. Tr. (Johansen) at 635.

74 Tr. (Johansen) at 620.

75 *Id.* at 620.

76 *Id.* at 621-22.

77 *Id.* at 621-22, 624; (Stevenson) at 214.

78 Tr. (Johansen) at 623.

79 Substantial questions have been raised both at trial and elsewhere as to the veracity of Mr. Johansen's claim. *See* Ex. CS, at S10006 ("Our analysis indicates that the primary technical breakthroughs were developed outside of the Linux development groups.").

the fact remains that Mr. Johansen created DeCSS in the full knowledge that it could be used on computers running Windows rather than Linux. Moreover, he was well aware that the files, once decrypted, could be copied like any other computer files.

In January 1999, Norwegian prosecutors filed charges against Mr. Johansen stemming from the development of DeCSS.[80] The disposition of the Norwegian case does not appear of record.

E. The Distribution of DeCSS

In the months following its initial appearance on Mr. Johansen's web site, DeCSS has become widely available on the Internet, where hundreds of sites now purport to offer the software for download.[81] A few other applications said to decrypt CSS-encrypted DVDs also have appeared on the Internet.[82]

In November 1999, defendants' web site began to offer DeCSS for download.[83] It established also a list of links to several web sites that purportedly "mirrored" or offered DeCSS for

---

80 Tr. (Johansen) at 626-27.

81 Ex. 97, 107, 126.

82 Tr. (Stevenson) at 217-18, 226-29; (Schumann) at 290, 338-41; (Johansen) at 641; (Reider) at 681-85. One, DOD (Drink or Die) Speed Ripper, does not work with all DVDs that DeCSS will decrypt. *Id.*; Ex. CS, at S10011; Ex. 9. Some of these programs perform only a portion of what DeCSS does and must be used in conjunction with others in order to decrypt the contents of a DVD. Tr. (Schuman) at 290, 338-39. Some of defendants' claims about these other means proved baseless at trial. *See* Tr. (Pavlovich) at 965-68.

83 Tr. (Corley) at 791; Ex. 28.

download.[84] The links on defendants' mirror list fall into one of three categories. By clicking the mouse on one of these links, the user may be brought to a page on the linked-to site on which there appears a further link to the DeCSS software.[85] If the user then clicks on the DeCSS link, download of the software begins. This page may or may not contain content other than the DeCSS link.[86] Alternatively, the user may be brought to a page on the linked-to site that does not itself purport to link to DeCSS, but that links, either directly or via a series of other pages on the site, to another page on the site on which there appears a link to the DeCSS software.[87] Finally, the user may be brought directly to the DeCSS link on the linked-to site such that download of DeCSS begins immediately without further user intervention.[88]

F. The Preliminary Injunction and Defendants' Response

The movie studios, through the Internet investigations division of the Motion Picture Association of America ("MPAA"), became aware of the availability of DeCSS on the Internet in

---

84 Tr. (Corley) at 791, 829, 848; Ex. 28.

85 Tr. (Corley) at 829-30, 845.

86 *Id.* at 831, 845.

87 *Id.* at 829-30, 845.

88 *Id.* at 830; (Shamos) at 38. As Mr. Corley testified, the download process generally begins with the appearance of a dialog box, or small window, prompting the user to confirm the location on the user's computer hard drive where the downloaded software will be stored. The actual download does not begin until the user provides the computer with this information. Tr. (Corley) at 830. It is possible also to create a link that commences the download immediately upon being clicked. *See* Tr. (Touretzky) at 1082-83.

October 1999.[89] The industry responded by sending out a number of cease and desist letters to web site operators who posted the software, some of which removed it from their sites.[90] In January 2000, the studios filed this lawsuit against defendant Eric Corley and two others.[91]

After a hearing at which defendants presented no affidavits or evidentiary material, the Court granted plaintiffs' motion for a preliminary injunction barring defendants from posting DeCSS.[92] At the conclusion of the hearing, plaintiffs sought also to enjoin defendants from linking to other sites that posted DeCSS, but the Court declined to entertain the application at that time in view of plaintiffs' failure to raise the issue in their motion papers.[93]

Following the issuance of the preliminary injunction, defendants removed DeCSS from the 2600.com web site.[94] In what they termed an act of "electronic civil disobedience,"[95] however, they continued to support links to other web sites purporting to offer DeCSS for download, a list

---

89 Tr. (Reider) at 652.

90 Tr. (King) at 435, 548; (Reider) at 653; Ex. 55.

91 The other two defendants entered into consent decrees with plaintiffs. Plaintiffs subsequently amended the complaint to add 2600 Enterprises, Inc. as a defendant.

92 Preliminary Injunction, Jan. 20, 2000 (DI 6); *Universal City Studios, Inc.*, 82 F. Supp.2d 211.

93 Tr., Jan. 20, 2000 (DI 17) at 85.

94 Tr. (Corley) at 791; Ex. 51.

95 Tr. (Corley) at 834; Ex. 96 (Corley Dep.) at 151-53.

which had grown to nearly five hundred by July 2000.[96] Indeed, they carried a banner saying "Stop the MPAA" and, in a reference to this lawsuit, proclaimed:

> "We have to face the possibility that we could be forced into submission. For that reason it's especially important that as many of you as possible, all throughout the world, take a stand and mirror these files."[97]

Thus, defendants obviously hoped to frustrate plaintiffs' recourse to the judicial system by making effective relief difficult or impossible.

At least some of the links currently on defendants' mirror list lead the user to copies of DeCSS that, when downloaded and executed, successfully decrypt a motion picture on a CSS-encrypted DVD.[98]

G. Effects on Plaintiffs

The effect on plaintiffs of defendants' posting of DeCSS depends upon the ease with which DeCSS decrypts plaintiffs' copyrighted motion pictures, the quality of the resulting product, and the convenience with which decrypted copies may be transferred or transmitted.

As noted, DeCSS was available for download from defendants' web site and remains available from web sites on defendants' mirror list.[99] Downloading is simple and quick—plaintiffs'

---

96 Tr. (Corley) at 791; Ex. 79 (Corley Dec.) ¶ 21; 126.

97 Ex. 106.

98 Tr. (Shamos) at 36-42; (Schumann) at 272-73; 265-66 (defendants' stipulation that their web site links to other sites containing executable copies of DeCSS).

99 Tr. (Shamos) at 36-42; (Schumann) at 272-73.

expert did it in seconds.[100] The program in fact decrypts at least some DVDs.[101] Although the process is computationally intensive, plaintiffs' expert decrypted a store-bought copy of *Sleepless in Seattle* in 20 to 45 minutes.[102] The copy is stored on the hard drive of the computer. The quality of the decrypted film is virtually identical to that of encrypted films on DVD.[103] The decrypted file can be copied like any other.[104]

The decryption of a CSS-protected DVD is only the beginning of the tale, as the decrypted file is very large—approximately 4.3 to 6 GB or more depending on the length of the film[105]—and thus extremely cumbersome to transfer or to store on portable storage media. One solution to this problem, however, is DivX, a compression utility available on the Internet that is promoted as a means of compressing decrypted motion picture files to manageable size.[106]

DivX is capable of compressing decrypted files constituting a feature length motion picture to approximately 650 MB at a compression ratio that involves little loss of quality.[107] While

---

100 Tr. (Shamos) at 39-40; *see also* Ex. AYZ (Hunt Dep.) at 18.

101 Tr. (Shamos) at 41-42; (Schumann) at 272-73.

102 Tr. (Shamos) at 41-42, 156.

103 Tr. (Schumann) at 273; Ex. AYZ (Hunt Dep.) at 26.

104 Tr. (Johansen) at 628; *see also* Ex. AZN (Simons Dep.) at 48.

105 Tr. (Shamos) at 42; (Ramadge) at 900.

106 *See* Tr. (Shamos) at 54-56; Ex. 112-13.

107 DivX effects what is known as "lossy" compression—it achieves its reduction in file size by eliminating some of the data in the file being compressed. The trick, however, is that it seeks

the compressed sound and graphic files then must be synchronized, a tedious process that took plaintiffs' expert between 10 and 20 hours,[108] the task is entirely feasible. Indeed, having compared a store-bought DVD with portions of a copy compressed and synchronized with DivX (which often are referred to as "DivX'd" motion pictures), the Court finds that the loss of quality, at least in some cases, is imperceptible or so nearly imperceptible as to be of no importance to ordinary consumers.[109]

The fact that DeCSS-decrypted DVDs can be compressed satisfactorily to 650 MB is very important. A writeable CD-ROM can hold 650 MB.[110] Hence, it is entirely feasible to decrypt a DVD with DeCSS, compress and synchronize it with DivX, and then make as many copies as one wishes by burning the resulting files onto writeable CD-ROMs, which are sold blank for about one dollar apiece.[111] Indeed, even if one wished to use a lower compression ratio to improve quality, a film easily could be compressed to about 1.3 GB and burned onto two CD-ROMs. But the creation of pirated copies of copyrighted movies on writeable CD-ROMs, although significant, is not the principal focus of plaintiffs' concern, which is transmission of pirated copies over the Internet or other

---

to do so by eliminating data that is imperceptible, or nearly so, to the human observer. Tr. (Shamos) at 43-44; (Ramadge) at 882-98.

108 Tr. (Shamos) at 51.

109 Defendants produced an expert whose DivX of a DeCSS decrypted file was of noticeably lower quality than that of plaintiffs' expert's DivX'd film. The reasons for the difference are not clear. The Court is satisfied, however, that it is possible to make high quality 650 MB DivX'd copies of many films.

110 Tr. (Ramadge) at 930.

111 Tr. (Shamos) at 56-57.

The copies do not require resynchronization of the sound and graphics.

networks.

Network transmission of decrypted motion pictures raises somewhat more difficult issues because even 650 MB is a very large file that, depending upon the circumstances, may take a good deal of time to transmit. But there is tremendous variation in transmission times. Many home computers today have modems with a rated capacity of 56 kilobits per second. DSL lines, which increasingly are available to home and business users, offer transfer rates of 7 megabits per second.[112] Cable modems also offer increased bandwidth. Student rooms in many universities are equipped with network connections rated at 10 megabits per second.[113] Large institutions such as universities and major companies often have networks with backbones rated at 100 megabits per second.[114] While effective transmission times generally are much lower than rated maximum capacities in consequence of traffic volume and other considerations, there are many environments in which very high transmission rates may be achieved.[115] Hence, transmission times ranging from three[116] to twenty minutes[117] to six hours[118] or more for a feature length film are readily achievable, depending upon the

---

112 Tr. (Shamos) at 95.

113 Tr. (Shamos) at 89-90, 98; (Peterson) at 865; (Pavlovich) at 943.

114 Tr. (Shamos) at 90; (Felten) at 772; (Peterson) at 879.

115 *See, e.g.,* Tr. (Peterson) at 861, 875-76.

116 *Id.* (Shamos) at 87-88.

117 *Id.*

118 *Id.* at 77.

users' precise circumstances.[119]

At trial, defendants repeated, as if it were a mantra, the refrain that plaintiffs, as they stipulated,[120] have no direct evidence of a specific occasion on which any person decrypted a copyrighted motion picture with DeCSS and transmitted it over the Internet. But that is unpersuasive. Plaintiffs' expert expended very little effort to find someone in an IRC chat room who exchanged a compressed, decrypted copy of *The Matrix*, one of plaintiffs' copyrighted motion pictures, for a copy of *Sleepless in Seattle*.[121] While the simultaneous electronic exchange of the two movies took approximately six hours,[122] the computers required little operator attention during the interim. An MPAA investigator downloaded between five and ten DVD-sourced movies over the Internet after December 1999.[123] At least one web site contains a list of 650 motion pictures, said to have been decrypted and compressed with DivX, that purportedly are available for sale, trade or free download.[124] And although the Court does not accept the list, which is hearsay, as proof of the truth of the matters asserted therein, it does note that advertisements for decrypted versions of

---

119 It should be noted here that the transmission time achieved by plaintiff's expert, Dr. Shamos, almost certainly was somewhat skewed because the work was done late at night on a university system after the close of the regular school year, conditions favorable to high effective transmission rates due to low traffic on the system.

120 Tr. (Schumann) at 334-36.

121 Tr. (Shamos) at 68-76.

122 *Id.* at 76-77.

123 Ex. AYY (Reider Dep.) at 98-101; *see also id.* at 121-23.

124 Ex. 116B.

copyrighted movies first appeared on the Internet in substantial numbers in late 1999, following the posting of DeCSS.[125]

The net of all this is reasonably plain. DeCSS is a free, effective and fast means of decrypting plaintiffs' DVDs and copying them to computer hard drives. DivX, which is available over the Internet for nothing, with the investment of some time and effort, permits compression of the decrypted files to sizes that readily fit on a writeable CD-ROM. Copies of such CD-ROMs can be produced very cheaply and distributed as easily as other pirated intellectual property. While not everyone with Internet access now will find it convenient to send or receive DivX'd copies of pirated motion pictures over the Internet, the availability of high speed network connections in many businesses and institutions, and their growing availability in homes, make Internet and other network traffic in pirated copies a growing threat.

These circumstances have two major implications for plaintiffs. First, the availability of DeCSS on the Internet effectively has compromised plaintiffs' system of copyright protection for DVDs, requiring them either to tolerate increased piracy or to expend resources to develop and implement a replacement system unless the availability of DeCSS is terminated.[126] It is analogous to the publication of a bank vault combination in a national newspaper. Even if no one uses the combination to open the vault, its mere publication has the effect of defeating the bank's security system, forcing the bank to reprogram the lock. Development and implementation of a new DVD copy protection system, however, is far more difficult and costly than reprogramming a combination

---

[125] Tr. (Reider) at 661.

[126] Tr. (King) at 418.

lock and may carry with it the added problem of rendering the existing installed base of compliant DVD players obsolete.

Second, the application of DeCSS to copy and distribute motion pictures on DVD, both on CD-ROMs and via the Internet, threatens to reduce the studios' revenue from the sale and rental of DVDs. It threatens also to impede new, potentially lucrative initiatives for the distribution of motion pictures in digital form, such as video-on-demand via the Internet.[127]

In consequence, plaintiffs already have been gravely injured. As the pressure for and competition to supply more and more users with faster and faster network connections grows, the injury will multiply.

II. The Digital Millennium Copyright Act

A. Background and Structure of the Statute

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 restrict acts, in respect of their works, which are not authorized by the authors concerned or permitted by law."[128]

---

127 *Id.* at 420.

128 WIPO Copyright Treaty, Apr. 12, 1997, Art. 11, S. Treaty Doc. No. 105-17 (1997), available at 1997 WL 447232.

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.[129] The DMCA was enacted in October 1998 as the culmination of this process.[130]

The DMCA contains two principal anticircumvention 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."[131] 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."[132] As defendants are accused here only of posting and linking to other sites posting DeCSS, and not of using it themselves to bypass plaintiffs' access controls, it is principally

---

129 There is an excellent account of the legislative history of the statute. Nimmer, *A Riff on Fair Use*, 148 U. PA. L. REV. at 702-38.

130 *See generally* S. REP. NO. 105-190, 105th Cong., 2d Sess. ("SENATE REP."), at 2-8 (1998).

131 H.R. REP. NO. 105-551(I), 105th Cong., 2d Sess. ("JUDICIARY COMM. REP."), at 17 (1998).

132 *Id.* at 18.

the second of the anticircumvention provisions that is at issue in this case.[133]

B. Posting of DeCSS

1. Violation of Anti-Trafficking Provision

Section 1201(a)(2) of the Copyright Act, part of the DMCA, provides that:

> "No person shall . . . offer to the public, provide or otherwise traffic in any technology . . . that—
>
> "(A) is primarily designed or produced for the purpose of circumventing a technological measure that effectively controls access to a work protected under [the Copyright Act];
>
> "(B) has only limited commercially significant purpose or use other than to circumvent a technological measure that effectively controls access to a work protected under [the Copyright Act]; or
>
> "(C) is marketed by that person or another acting in concert with that person with that person's knowledge for use in circumventing a technological measure that effectively controls access to a work protected under [the Copyright Act]."[134]

In this case, defendants concededly offered and provided and, absent a court order, would continue to offer and provide DeCSS to the public by making it available for download on the 2600.com web site. DeCSS, a computer program, unquestionably is "technology" within the meaning

---

133 Plaintiffs rely also on Section 1201(b), which is very similar to Section 1201(a)(2) except that the former applies to trafficking in means of circumventing protection offered by a technological measure that effectively protects "a right of a copyright owner in a work or a portion thereof" whereas the latter applies to trafficking in means of circumventing measures controlling access to a work. *See generally* 1 MELVILLE B. NIMMER & DAVID NIMMER, NIMMER ON COPYRIGHT ("NIMMER") § 12A.03[C] (1999). In addition, as noted below, certain of the statutory exceptions upon which defendants have relied apply only to Section 1201(a)(2).

134 17 U.S.C. § 1201(a)(2). *See also* 1 NIMMER § 12A.03[1][*a*], at 12A-16.

of the statute.[135] "[C]ircumvent a technological measure" is defined to mean descrambling a scrambled work, decrypting an encrypted work, or "otherwise to avoid, bypass, remove, deactivate, or impair a technological measure, without the authority of the copyright owner,"[136] so DeCSS clearly is a means of circumventing a technological access control measure.[137] In consequence, if CSS otherwise falls within paragraphs (A), (B) or (C) of Section 1201(a)(2), and if none of the statutory exceptions applies to their actions, defendants have violated and, unless enjoined, will continue to violate the DMCA by posting DeCSS.

---

135 In their Post-Trial Brief, defendants argue that "at least some of the members of Congress" understood § 1201 to be limited to conventional devices, specifically 'black boxes,' as opposed to computer code." Def. Post-Trial Mem. at 21. However, the statute is clear that it prohibits "*any technology*," not simply black boxes. 17 U.S.C. § 1201(a)(2) (emphasis added).

136 17 U.S.C. § 1201(a)(3)(A).

137 Decryption or avoidance of an access control measure is not "circumvention" within the meaning of the statute unless it occurs "without the authority of the copyright owner." 17 U.S.C. § 1201(a)(3)(A). Defendants posit that purchasers of a DVD acquire the right "to perform all acts with it that are not exclusively granted to the copyright holder." Based on this premise, they argue that DeCSS does not circumvent CSS within the meaning of the statute because the Copyright Act does not grant the copyright holder the right to prohibit purchasers from decrypting. As the copyright holder has no statutory right to prohibit decryption, the argument goes, decryption cannot be understood as unlawful circumvention. Def. Post-Trial Mem. 10-13. The argument is pure sophistry. The DMCA proscribes trafficking in technology that decrypts or avoids an access control measure without the copyright holder consenting to the decryption or avoidance. *See* JUDICIARY COMM. REP. at 17-18 (fair use applies "where the access is authorized"). Defendants' argument seems to be a corruption of the first sale doctrine, which holds that the copyright holder, notwithstanding the exclusive distribution right conferred by Section 106(3) of the Copyright Act, 17 U.S.C. § 106(3), is deemed by its "first sale" of a copy of the copyrighted work to have consented to subsequent sale of the copy. *See generally* 2 NIMMER §§ 8.11-8.12.

a. Section 1201(a)(2)(A)

(1) CSS Effectively Controls Access to Copyrighted Works

During pretrial proceedings and at trial, defendants attacked plaintiffs' Section 1201(a)(2)(A) claim, arguing that CSS, which is based on a 40-bit encryption key, is a weak cipher that does not "effectively control" access to plaintiffs' copyrighted works. They reasoned from this premise that CSS is not protected under this branch of the statute at all. Their post-trial memorandum appears to have abandoned this argument. In any case, however, the contention is indefensible as a matter of law.

First, the statute expressly provides that "a technological measure 'effectively controls access to a work' if the measure, 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 a work."[138] One cannot gain access to a CSS-protected work on a DVD without application of the three keys that are required by the software. One cannot lawfully gain access to the keys except by entering into a license with the DVD CCA under authority granted by the copyright owners or by purchasing a DVD player or drive containing the keys pursuant to such a license. In consequence, under the express terms of the statute, CSS "effectively controls access" to copyrighted DVD movies. It does so, within the meaning of the statute, whether or not it is a strong means of protection.[139]

This view is confirmed by the legislative history, which deals with precisely this point. The House Judiciary Committee section-by-section analysis of the House bill, which in this respect

---

138 *Id.* § 1201(a)(3)(B).

139 *RealNetworks, Inc. v. Streambox, Inc.*, No. 2:99CV02070, 2000 WL 127311, *9 (W.D. Wash. Jan. 18, 2000).

was enacted into law, makes clear that a technological measure "effectively controls access" to a copyrighted work if its *function* is to control access:

> "The bill does define the *functions* of the technological measures that are covered—that is, what it means for a technological measure to 'effectively control access to a work' . . . and to 'effectively protect a right of a copyright owner under this title' . . . . The practical, common-sense approach taken by H.R. 2281 is that if, in the ordinary course of its operation, a technology actually works in the defined ways to control access to a work . . . then the 'effectiveness' test is met, and the prohibitions of the statute are applicable. This test, which focuses on the function performed by the technology, provides a sufficient basis for clear interpretation."[140]

Further, the House Commerce Committee made clear that measures based on encryption or scrambling "effectively control" access to copyrighted works,[141] although it is well known that what may be encrypted or scrambled often may be decrypted or unscrambled. As CSS, in the ordinary course of its operation—that is, when DeCSS or some other decryption program is not employed—"actually works" to prevent access to the protected work, it "effectively controls access" within the contemplation of the statute.

Finally, the interpretation of the phrase "effectively controls access" offered by defendants at trial—viz., that the use of the word "effectively" means that the statute protects only successful or efficacious technological means of controlling access—would gut the statute if it were adopted. If a technological means of access control is circumvented, it is, in common parlance, ineffective. Yet defendants' construction, if adopted, would limit the application of the statute to access control measures that thwart circumvention, but withhold protection for those measures that

---

140 HOUSE COMM. ON JUDICIARY, SECTION-BY-SECTION ANALYSIS OF H.R. 2281 AS PASSED BY THE UNITED STATES HOUSE OF REPRESENTATIVES ON AUGUST 4, 1998 ("SECTION-BY-SECTION ANALYSIS"), at 10 (Comm. Print 1998) (emphasis in original).

141 H.R. REP. NO. 105-551(II), 105th Cong., 2d Sess. ("COMMERCE COMM. REP."), at 39 (1998).

can be circumvented. In other words, defendants would have the Court construe the statute to offer protection where none is needed but to withhold protection precisely where protection is essential. The Court declines to do so. Accordingly, the Court holds that CSS effectively controls access to plaintiffs' copyrighted works.[142]

(2) DeCSS Was Designed Primarily to Circumvent CSS

As CSS effectively controls access to plaintiffs' copyrighted works, the only remaining question under Section 1201(a)(2)(A) is whether DeCSS was designed primarily to circumvent CSS. The answer is perfectly obvious. By the admission of both Jon Johansen, the programmer who principally wrote DeCSS, and defendant Corley, DeCSS was created solely for the purpose of decrypting CSS—that is all it does.[143] Hence, absent satisfaction of a statutory exception, defendants clearly violated Section 1201(a)(2)(A) by posting DeCSS to their web site.

b. Section 1201(a)(2)(B)

As the only purpose or use of DeCSS is to circumvent CSS, the foregoing is sufficient to establish a *prima facie* violation of Section 1201(a)(2)(B) as well.

c. The Linux Argument

---

142 Defendants, in a reprise of their argument that DeCSS is not a circumvention device, argue also that CSS does not effectively control access to copyrighted works within the meaning of the statute because plaintiffs authorize avoidance of CSS by selling their DVDs. Def. Post-Trial Mem. 10-13. The argument is specious in this context as well. *See supra* note 137.

143 Tr. (Johansen) at 619; (Corley) 833-34.

Perhaps the centerpiece of defendants' statutory position is the contention that DeCSS was not created for the purpose of pirating copyrighted motion pictures. Rather, they argue, it was written to further the development of a DVD player that would run under the Linux operating system, as there allegedly were no Linux compatible players on the market at the time.[144] The argument plays itself out in various ways as different elements of the DMCA come into focus. But it perhaps is useful to address the point at its most general level in order to place the preceding discussion in its fullest context.

As noted, Section 1201(a) of the DMCA contains two distinct prohibitions. Section 1201(a)(1), the so-called basic provision, "aims against those who engage in unauthorized circumvention of technological measures . . . . [It] focuses directly on wrongful conduct, rather than on those who facilitate wrongful conduct . . . ."[145] Section 1201(a)(2), the anti-trafficking provision at issue in this case, on the other hand, separately bans offering or providing technology that may be used to circumvent technological means of controlling access to copyrighted works.[146] If the means in question meets any of the three prongs of the standard set out in Section 1201(a)(2)(A), (B), or (C), it may not be offered or disseminated.

As the earlier discussion demonstrates, the question whether the development of a Linux DVD player motivated those who wrote DeCSS is immaterial to the question whether the defendants now before the Court violated the anti-trafficking provision of the DMCA. The

---

144 Def. Post-Trial Mem. at 2.

145 1 NIMMER § 12A.03[A], at 12A-15 (1999 Supp.).

146 *See id.* § 12A.03[B], at 12A-25 to 12A-26.

inescapable facts are that (1) CSS is a technological means that effectively controls access to plaintiffs' copyrighted works, (2) the one and only function of DeCSS is to circumvent CSS, and (3) defendants offered and provided DeCSS by posting it on their web site. Whether defendants did so in order to infringe, or to permit or encourage others to infringe, copyrighted works in violation of other provisions of the Copyright Act simply does not matter for purposes of Section 1201(a)(2). The offering or provision of the program is the prohibited conduct—and it is prohibited irrespective of why the program was written, except to whatever extent motive may be germane to determining whether their conduct falls within one of the statutory exceptions.

2. Statutory Exceptions

Earlier in the litigation, defendants contended that their activities came within several exceptions contained in the DMCA and the Copyright Act and constitute fair use under the Copyright Act. Their post-trial memorandum appears to confine their argument to the reverse engineering exception.[147] In any case, all of their assertions are entirely without merit.

a. Reverse engineering

Defendants claim to fall under Section 1201(f) of the statute, which provides in substance that one may circumvent, or develop and employ technological means to circumvent, access control measures in order to achieve interoperability with another computer program provided

---

[147] *See* Def. Post-Trial Mem. at 13.

that doing so does not infringe another's copyright[148] and, in addition, that one may make information acquired through such efforts "available to others, if the person [in question] . . . provides such information solely for the purpose of enabling interoperability of an independently created computer program with other programs, and to the extent that doing so does not constitute infringement . . . ."[149] They contend that DeCSS is necessary to achieve interoperability between computers running the Linux operating system and DVDs and that this exception therefore is satisfied.[150] This contention fails.

First, Section 1201(f)(3) permits information acquired through reverse engineering to be made available to others only by the person who acquired the information. But these defendants did not do any reverse engineering. They simply took DeCSS off someone else's web site and posted it on their own.

Defendants would be in no stronger position even if they had authored DeCSS. The right to make the information available extends only to dissemination "solely for the purpose" of achieving interoperability as defined in the statute. It does not apply to public dissemination of means of circumvention, as the legislative history confirms.[151] These defendants, however, did not post DeCSS "solely" to achieve interoperability with Linux or anything else.

Finally, it is important to recognize that even the creators of DeCSS cannot credibly

---

148 17 U.S.C. §§ 1201(f)(1), (2).

149 *Id.* § 1201(f)(3).

150 Def. Post-Trial Mem. at 13-15.

151 COMMERCE COMM. REP. at 43.

maintain that the "sole" purpose of DeCSS was to create a Linux DVD player. DeCSS concededly was developed on and runs under Windows—a far more widely used operating system. The developers of DeCSS therefore knew that DeCSS could be used to decrypt and play DVD movies on Windows as well as Linux machines. They knew also that the decrypted files could be copied like any other unprotected computer file. Moreover, the Court does not credit Mr. Johansen's testimony that he created DeCSS solely for the purpose of building a Linux player. Mr. Johansen is a very talented young man and a member of a well known hacker group who viewed "cracking" CSS as an end it itself and a means of demonstrating his talent and who fully expected that the use of DeCSS would not be confined to Linux machines. Hence, the Court finds that Mr. Johansen and the others who actually did develop DeCSS did not do so solely for the purpose of making a Linux DVD player if, indeed, developing a Linux-based DVD player was among their purposes.

Accordingly, the reverse engineering exception to the DMCA has no application here.

b. Encryption research

Section 1201(g)(4) provides in relevant part that:

> "Notwithstanding the provisions of subsection (a)(2), it is not a violation of that subsection for a person to—
>
> "(A) develop and employ technological means to circumvent a technological measure for the sole purpose of that person performing the acts of good faith encryption research described in paragraph (2); and
>
> "(B) provide the technological means to another person with whom he or she is working collaboratively for the purpose of conducting the acts of good faith encryption research described in paragraph (2) or for the purpose of having that other person verify his or her acts of good faith encryption research described in paragraph

(2)."[152]

Paragraph (2) in relevant part permits circumvention of technological measures in the course of good faith encryption research if:

> "(A) the person lawfully obtained the encrypted copy, phonorecord, performance, or display of the published work;
>
> "(B) such act is necessary to conduct such encryption research;
>
> "(C) the person made a good faith effort to obtain authorization before the circumvention; and
>
> "(D) such act does not constitute infringement under this title . . . ."[151]

In determining whether one is engaged in good faith encryption research, the Court is instructed to consider factors including whether the results of the putative encryption research are disseminated in a manner designed to advance the state of knowledge of encryption technology versus facilitation of copyright infringement, whether the person in question is engaged in legitimate study of or work in encryption, and whether the results of the research are communicated in a timely fashion to the copyright owner.[152]

Neither of the defendants remaining in this case was or is involved in good faith encryption research.[153] They posted DeCSS for all the world to see. There is no evidence that they made any effort to provide the results of the DeCSS effort to the copyright owners. Surely there is

---

[152] 17 U.S.C. § 1201(g)(4).

[151] *Id.* § 1201(g)(2).

[152] *Id.* § 1201(g)(3).

[153] Ex. 96 (Corley Dep.) at 33.

no suggestion that either of them made a good faith effort to obtain authorization from the copyright owners. Accordingly, defendants are not protected by Section 1201(g).[154]

c. Security testing

Defendants contended earlier that their actions should be considered exempt security testing under Section 1201(j) of the statute.[155] This exception, however, is limited to "assessing a computer, computer system, or computer network, solely for the purpose of good faith testing, investigating, or correcting [of a] security flaw or vulnerability, with the authorization of the owner or operator of such computer system or computer network."[156]

The record does not indicate that DeCSS has anything to do with testing computers, computer systems, or computer networks. Certainly defendants sought, and plaintiffs' granted, no authorization for defendants' activities. This exception therefore has no bearing in this case.[157]

d. Fair use

Finally, defendants rely on the doctrine of fair use. Stated in its most general terms,

---

154 In any case, Section 1201(g), where its requirements are met, is a defense only to claims under Section 1201(a)(2), not those under Section 1201(b).

155 Def. Mem. in Opp. to Prelim. Inj. (DI 11) at 11-12.

156 *Id.* § 1201(j)(1).

157 Like Section 1201(g), moreover, Section 1201(j) provides no defense to a Section 1201(b) claim.

the doctrine, now codified in Section 107 of the Copyright Act,[158] limits the exclusive rights of a copyright holder by permitting others to make limited use of portions of the copyrighted work, for appropriate purposes, free of liability for copyright infringement. For example, it is permissible for one other than the copyright owner to reprint or quote a suitable part of a copyrighted book or article in certain circumstances. The doctrine traditionally has facilitated literary and artistic criticism, teaching and scholarship, and other socially useful forms of expression. It has been viewed by courts as a safety valve that accommodates the exclusive rights conferred by copyright with the freedom of expression guaranteed by the First Amendment.

The use of technological means of controlling access to a copyrighted work may affect the ability to make fair uses of the work.[159] Focusing specifically on the facts of this case, the application of CSS to encrypt a copyrighted motion picture requires the use of a compliant DVD player to view or listen to the movie. Perhaps more significantly, it prevents exact copying of either the video or the audio portion of all or any part of the film.[160] This latter point means that certain uses

---

158

17 U.S.C. § 107.

159

Indeed, as many have pointed out, technological means of controlling access to works create a risk, depending upon future technological and commercial developments, of limiting access to works that are not protected by copyright such as works upon which copyright has expired. *See, e.g.,* Nimmer, *A Riff on Fair Use,* 148 U. PA. L. REV. at 738-40; Hannibal Travis, *Comment, Pirates of the Information Infrastrcuture: Blackstonian Copyright and the First Amendment,* 15 BERKELEY TECH. L. J. 777, 861 (2000) (hereinafter *Pirates of the Information Infrastructure*); Yochai Benkler, *Free as the Air to Common Use: First Amendment Constraints on Enclosure of the Public Domain,* 74 N.Y.U. L. REV. 354, 421 (1999);

160

Of course, one might quote the verbal portion of the sound track, rerecord both verbal and nonverbal portions of the sound track, and video tape or otherwise record images produced on a monitor when the DVD is played on a compliant DVD player.

that might qualify as "fair" for purposes of copyright infringement—for example, the preparation by a film studies professor of a single CD-ROM or tape containing two scenes from different movies in order to illustrate a point in a lecture on cinematography, as opposed to showing relevant parts of two different DVDs—would be difficult or impossible absent circumvention of the CSS encryption. Defendants therefore argue that the DMCA cannot properly be construed to make it difficult or impossible to make any fair use of plaintiffs' copyrighted works and that the statute therefore does not reach their activities, which are simply a means to enable users of DeCSS to make such fair uses.

Defendants have focused on a significant point. Access control measures such as CSS do involve some risk of preventing lawful as well as unlawful uses of copyrighted material. Congress, however, clearly faced up to and dealt with this question in enacting the DMCA.

The Court begins its statutory analysis, as it must, with the language of the statute. Section 107 of the Copyright Act provides in critical part that certain uses of copyrighted works that otherwise would be wrongful are "not . . . infringement[s] of copyright."[161] Defendants, however, are not here sued for copyright infringement. They are sued for offering and providing technology designed to circumvent technological measures that control access to copyrighted works and otherwise violating Section 1201(a)(2) of the Act. If Congress had meant the fair use defense to apply to such actions, it would have said so. Indeed, as the legislative history demonstrates, the decision not to make fair use a defense to a claim under Section 1201(a) was quite deliberate.

Congress was well aware during the consideration of the DMCA of the traditional role of the fair use defense in accommodating the exclusive rights of copyright owners with the legitimate

---

[161] 17 U.S.C. § 107.

interests of noninfringing users of portions of copyrighted works. It recognized the contention, voiced by a range of constituencies concerned with the legislation, that technological controls on access to copyrighted works might erode fair use by preventing access even for uses that would be deemed "fair" if only access might be gained.[162] And it struck a balance among the competing interests.

The first element of the balance was the careful limitation of Section 1201(a)(1)'s prohibition of the act of circumvention to the act itself so as not to "apply to subsequent actions of a person once he or she has obtained authorized access to a copy of a [copyrighted] work . . . ."[163] By doing so, it left "the traditional defenses to copyright infringement, including fair use, . . . fully applicable" provided "the access is authorized."[164]

Second, Congress delayed the effective date of Section 1201(a)(1)'s prohibition of the act of circumvention for two years pending further investigation about how best to reconcile Section 1201(a)(1) with fair use concerns. Following that investigation, which is being carried out in the form of a rule-making by the Register of Copyright, the prohibition will not apply to users of particular classes of copyrighted works who demonstrate that their ability to make noninfringing uses of those classes of works would be affected adversely by Section 1201(a)(1).[165]

---

162 *See, e.g.,* COMMERCE COMM. REP. 25-26.

163 JUDICIARY COMM. REP. 18.

164 *Id.*

165 17 U.S.C. §§ 1201(a)(1)(B)-(E).

The rule-making is under way. 65 F.R. 14505-06 (Mar. 17, 2000); *see also*

Third, it created a series of exceptions to aspects of Section 1201(a) for certain uses that Congress thought "fair," including reverse engineering, security testing, good faith encryption research, and certain uses by nonprofit libraries, archives and educational institutions.[166]

Defendants claim also that the possibility that DeCSS might be used for the purpose of gaining access to copyrighted works in order to make fair use of those works saves them under *Sony Corp. v. Universal City Studios, Inc.*[167] But they are mistaken. *Sony* does not apply to the activities with which defendants here are charged. Even if it did, it would not govern here. *Sony* involved a construction of the Copyright Act that has been overruled by the later enactment of the DMCA to the extent of any inconsistency between *Sony* and the new statute.

Sony was a suit for contributory infringement brought against manufacturers of video cassette recorders on the theory that the manufacturers were contributing to infringing home taping of copyrighted television broadcasts. The Supreme Court held that the manufacturers were not liable in view of the substantial numbers of copyright holders who either had authorized or did not object to such taping by viewers.[168] But *Sony* has no application here.

When *Sony* was decided, the only question was whether the manufacturers could be held liable for infringement by those who purchased equipment from them in circumstances in which there were many noninfringing uses for their equipment. But that is not the question now before this

---

<http://www.loc.gov/copyright/1201/anticirc.html> (visited July 28, 2000).

166 17 U.S.C. §§ 1201(d), (f), (g), (j).

167 464 U.S. 417 (1984).

168 *Id.* at 443, 446.

Court. The question here is whether the possibility of noninfringing fair use by someone who gains access to a protected copyrighted work through a circumvention technology distributed by the defendants saves the defendants from liability under Section 1201. But nothing in Section 1201 so suggests. By prohibiting the provision of circumvention technology, the DMCA fundamentally altered the landscape. A given device or piece of technology might have "a substantial noninfringing use, and hence be immune from attack under *Sony*'s construction of the Copyright Act—but nonetheless still be subject to suppression under Section 1201."[169] Indeed, Congress explicitly noted that Section 1201 does not incorporate *Sony*.[170]

The policy concerns raised by defendants were considered by Congress. Having considered them, Congress crafted a statute that, so far as the applicability of the fair use defense to Section 1201(a) claims is concerned, is crystal clear. In such circumstances, courts may not undo what Congress so plainly has done by "construing" the words of a statute to accomplish a result that Congress rejected. The fact that Congress elected to leave technologically unsophisticated persons who wish to make fair use of encrypted copyrighted works without the technical means of doing so is a matter for Congress unless Congress' decision contravenes the Constitution, a matter to which the Court turns below. Defendants' statutory fair use argument therefore is entirely without merit.

---

169 *RealNetworks, Inc.*, 2000 WL 127311, at *8 (quoting 1 NIMMER § 12A.18[B], at 12A-130) (internal quotation marks omitted).

170 SECTION-BY-SECTION ANALYSIS 9 ("The *Sony* test of 'capab[ility] of substantial non-infringing uses,' while still operative in cases claiming contributory infringement of copyright, is not part of this legislation . . . .").

C. Linking to Sites Offering DeCSS

Plaintiffs seek also to enjoin defendants from "linking" their 2600.com web site to other sites that make DeCSS available to users. Their request obviously stems in no small part from what defendants themselves have termed their act of "electronic civil disobedience"—their attempt to defeat the purpose of the preliminary injunction by (a) offering the practical equivalent of making DeCSS available on their own web site by electronically linking users to other sites still offering DeCSS, and (b) encouraging other sites that had not been enjoined to offer the program. The dispositive question is whether linking to another web site containing DeCSS constitutes "offer[ing DeCSS] to the public" or "provid[ing] or otherwise traffic[king]" in it within the meaning of the DMCA.[171] Answering this question requires careful consideration of the nature and types of linking.

Most web pages are written in computer languages, chiefly HTML, which allow the programmer to prescribe the appearance of the web page on the computer screen and, in addition, to instruct the computer to perform an operation if the cursor is placed over a particular point on the screen and the mouse then clicked.[172] Programming a particular point on a screen to transfer the user to another web page when the point, referred to as a hyperlink, is clicked is called linking.[173] Web pages can be designed to link to other web pages on the same site or to web pages maintained by

---

[171] 17 U.S.C. § 1201(a)(2).

[172] Tr. (Schumann) at 275-76.

[173] *Id.* at 261-62.

different sites.[174]

As noted earlier, the links that defendants established on their web site are of several types. Some transfer the user to a web page on an outside site that contains a good deal of information of various types, does not itself contain a link to DeCSS, but that links, either directly or via a series of other pages, to another page on the same site that posts the software. It then is up to the user to follow the link or series of links on the linked-to web site in order to arrive at the page with the DeCSS link and commence the download of the software. Others take the user to a page on an outside web site on which there appears a direct link to the DeCSS software and which may or may not contain text or links other than the DeCSS link. The user has only to click on the DeCSS link to commence the download. Still others may directly transfer the user to a file on the linked-to web site such that the download of DeCSS to the user's computer automatically commences without further user intervention.

The statute makes it unlawful to offer, provide or otherwise traffic in described technology.[175] To "traffic" in something is to engage in dealings in it,[176] conduct that necessarily involves awareness of the nature of the subject of the trafficking. To "provide" something, in the sense used in the statute, is to make it available or furnish it.[177] To "offer" is to present or hold it out

---

174 For example, a web page maintained by a radio station might provide a hyperlink to a weather report by programming its page to transfer the user to a National Weather Service site if the user clicks on the "weather" hyperlink.

175 17 U.S.C. § 1201(a)(2).

176 *See* 2 THE COMPACT EDITION OF THE OXFORD ENGLISH DICTIONARY 3372 (1971).

177 *See* 2 *id.* 2340.

for consideration.[178] The phrase "or otherwise traffic in" modifies and gives meaning to the words "offer" and "provide."[179] In consequence, the anti-trafficking provision of the DMCA is implicated where one presents, holds out or makes a circumvention technology or device available, knowing its nature, for the purpose of allowing others to acquire it.

To the extent that defendants have linked to sites that automatically commence the process of downloading DeCSS upon a user being transferred by defendants' hyperlinks, there can be no serious question. Defendants are engaged in the functional equivalent of transferring the DeCSS code to the user themselves.

Substantially the same is true of defendants' hyperlinks to web pages that display nothing more than the DeCSS code or present the user only with the choice of commencing a download of DeCSS and no other content. The only distinction is that the entity extending to the user the option of downloading the program is the transferee site rather than defendants, a distinction without a difference.

Potentially more troublesome might be links to pages that offer a good deal of content other than DeCSS but that offer a hyperlink for downloading, or transferring to a page for downloading, DeCSS. If one assumed, for the purposes of argument, that the *Los Angeles Times* web site somewhere contained the DeCSS code, it would be wrong to say that anyone who linked to the *Los Angeles Times* web site, regardless of purpose or the manner in which the link was described, thereby offered, provided or otherwise trafficked in DeCSS merely because DeCSS

---

178 *See* 1 *id.* 1979.

179 *See, e.g.*, *Strom v. Goldman, Sachs & Co.*, 202 F.3d 138, 146-47 (2d Cir. 1999).

happened to be available on a site to which one linked.[180] But that is not this case. Defendants urged others to post DeCSS in an effort to disseminate DeCSS and to inform defendants that they were doing so. Defendants then linked their site to those "mirror" sites, after first checking to ensure that the mirror sites in fact were posting DeCSS or something that looked like it, and proclaimed on their own site that DeCSS could be had by clicking on the hyperlinks on defendants' site. By doing so, they offered, provided or otherwise trafficked in DeCSS, and they continue to do so to this day.

III. The First Amendment

Defendants argue that the DMCA, at least as applied to prevent the public dissemination of DeCSS, violates the First Amendment to the Constitution. They claim that it does so in two ways. First, they argue that computer code is protected speech and that the DMCA's prohibition of dissemination of DeCSS therefore violates defendants' First Amendment rights. Second, they contend that the DMCA is unconstitutionally overbroad, chiefly because its prohibition of the dissemination of decryption technology prevents third parties from making fair use of plaintiffs' encrypted works, and vague. They argue also that a prohibition on their linking to sites that make DeCSS available is unconstitutional for much the same reasons.

A. Computer Code and the First Amendment

The premise of defendants' first position is that computer code, the form in which

---

180 *See DVD Copy Control Ass'n, Inc. v. McLaughlin*, No. CV 786804, 2000 WL 48512, *4 (Cal. Super. Jan. 21, 2000) ("website owner cannot be held responsible for all of the content of the sites to which it provides links"); Richard Raysman & Peter Brown, *Recent Linking Issues*, N.Y.L.J., Feb. 8, 2000, p. 3, col. 1 (same).

DeCSS exists, is speech protected by the First Amendment. Examination of that premise is the logical starting point for analysis. And it is important in examining that premise first to define terms.

Defendants' assertion that computer code is "protected" by the First Amendment is quite understandable. Courts often have spoken of certain categories of expression as "not within the area of constitutionally protected speech,"[181] so defendants naturally wish to avoid exclusion by an unfavorable categorization of computer code. But such judicial statements in fact are not literally true. All modes of expression are covered by the First Amendment in the sense that the constitutionality of their "regulation must be determined by reference to First Amendment doctrine and analysis."[182] Regulation of different categories of expression, however, is subject to varying levels of judicial scrutiny. Thus, to say that a particular form of expression is "protected" by the First Amendment means that the constitutionality of any regulation of it must be measured by reference to the First Amendment. In some circumstances, however, the phrase connotes also that the standard for measurement is the most exacting level available.

It cannot seriously be argued that any form of computer code may be regulated without reference to First Amendment doctrine. The path from idea to human language to source code to object code is a continuum. As one moves from one to the other, the levels of precision and,

---

181 *Roth v. United States*, 354 U.S. 476, 483 (1957) (obscenity). *See also, e.g.*, *Sable Comm. of Cal., Inc. v. FCC*, 492 U.S. 115, 124 (1989) (obscenity); *Bose Corp. v. Consumers Union of United States*, 466 U.S. 485, 504 (1984) (libel, obscenity, fighting words, child pornography); *Beauharnais v. Illinois*, 343 U.S. 250, 266 (1952) (defamation); *Chaplinsky v. New Hampshire*, 315 U.S. 568, 571-72 (1942) (fighting words).

182 Robert Post, *Encryption Source Code and the First Amendment*, 15 BERKELEY TECH. L. J. 713, 714 (2000); *see R.A.V. v. City of St. Paul, Minnesota*, 505 U.S. 373, 382 (1992) (statements that categories of speech are "unprotected" are not literally true; characterization indicates only that they are subject to content based regulation).

arguably, abstraction increase, as does the level of training necessary to discern the idea from the expression. Not everyone can understand each of these forms. Only English speakers will understand English formulations. Principally those familiar with the particular programming language will understand the source code expression. And only a relatively small number of skilled programmers and computer scientists will understand the machine readable object code. But each form expresses the same idea, albeit in different ways.[183]

There perhaps was a time when the First Amendment was viewed only as a limitation on the ability of government to censor speech in advance.[184] But we have moved far beyond that. All modes by which ideas may be expressed or, perhaps, emotions evoked—including speech, books, movies, art, and music—are within the area of First Amendment concern.[185] As computer code—whether source or object—is a means of expressing ideas, the First Amendment must be considered before its dissemination may be prohibited or regulated. In that sense, computer code is covered or, as sometimes is said, "protected" by the First Amendment.[186] But that conclusion still

---

183 The Court is indebted to Professor David Touretzky of Carnegie-Mellon University, who testified on behalf of defendants, for his lucid explication of this point. *See* Tr. (Touretzky) at 1066-84 & Ex. BBE, CCO, CCP, CCQ. As will appear, however, the point does not lead the Court to the same conclusion as Dr. Touretzky.

184 LEONARD LEVY, FREEDOM OF SPEECH IN EARLY AMERICAN HISTORY: LEGACY OF SUPPRESSION *passim* (1960); *see also* 4 RONALD D. ROTUNDA & JOHN E. NOWAK, TREATISE ON CONSTITUTIONAL LAW § 20.5 (1999); 4 WILLIAM BLACKSTONE, COMMENTARIES ON THE LAWS OF ENGLAND 151-52 (1769).

185 *See, e.g.*, *Hurley v. Irish-American Gay, Lesbian and Bisexual Group*, 515 U.S. 557, 569 (1995).

186 *Junger v. Daley*, 209 F.3d 481, 485 (6th Cir. 2000); *Bernstein v. U.S. Dept. of State*, 176 F.3d 1132, 1141, *reh'g granted and opinion withdrawn*, 192 F.3d 1308 (9th Cir. 1999); *Bernstein v. U.S. Dept. of State*, 922 F. Supp. 1426, 1436 (N.D. Cal. 1996) (First

leaves for determination the level of scrutiny to be applied in determining the constitutionality of regulation of computer code.

B. The Constitutionality of the DMCA's Anti-Trafficking Provision

1. Defendants' Alleged Right to Disseminate DeCSS

Defendants first attack Section 1201(a)(2), the anti-trafficking provision, as applied to them on the theory that DeCSS is constitutionally protected expression and that the statute improperly prevents them from communicating it. Their attack presupposes that a characterization of code as constitutionally protected subjects any regulation of code to the highest level of First Amendment scrutiny. As we have seen, however, this does not necessarily follow.

Just as computer code cannot be excluded from the area of First Amendment concern because it is abstract and, in many cases, arcane, the long history of First Amendment jurisprudence makes equally clear that the fact that words, symbols and even actions convey ideas and evoke emotions does not inevitably place them beyond the power of government. The Supreme Court has evolved an analytical framework by which the permissibility of particular restrictions on the expression of ideas must determined.

Broadly speaking, restrictions on expression fall into two categories. Some are restrictions on the voicing of particular ideas, which typically are referred to as content based restrictions. Others have nothing to do with the content of the expression—i.e., they are content neutral—but they have the incidental effect of limiting expression.

Amendment extends to source code); *see Karn v. U.S. Dept. of State*, 925 F.2d 1, 10 (D. D.C. 1996) (assuming First Amendment extends to source code).

In general, "government has no power to restrict expression because of its message, its ideas, its subject matter, or its content . . . ."[187] "[S]ubject only to narrow and well-understood exceptions, [the First Amendment] does not countenance governmental control over the content of messages expressed by private individuals."[188] In consequence, content based restrictions on speech are permissible only if they serve compelling state interests by the least restrictive means available.[189]

Content neutral restrictions, in contrast, are measured against a less exacting standard. Because restrictions of this type are not motivated by a desire to limit the message, they will be upheld if they serve a substantial governmental interest and restrict First Amendment freedoms no more than necessary.[190]

Restrictions on the nonspeech elements of expressive conduct fall into the conduct-neutral category. The Supreme Court long has distinguished for First Amendment purposes between pure speech, which ordinarily receives the highest level of protection, and expressive conduct.[191]

---

187 *Police Department of the City of Chicago v. Mosely*, 408 U.S. 92, 95-96 (1972).

188 *Turner Broadcasting System, Inc. v. FCC*, 512 U.S. 622, 641 (1994); *accord, R.A.V.*, 505 U.S. at 382-83.

189 *Sable Comm. of Cal., Inc. v. FCC*, 492 U.S. at 126.

190 *Turner Broadcasting System, Inc.*, 512 U.S. at 662 (citing *United States v. O'Brien*, 391 U.S. 367, 377 (1968)).

191 *See, e.g., United States v. O'Brien*, 391 U.S. at 376.

Even if conduct contains an expressive element, its nonspeech aspect need not be ignored.[192] "[W]hen 'speech' and 'nonspeech' elements are combined in the same course of conduct, a sufficiently important governmental interest in regulating the nonspeech element can justify incidental limitations on First Amendment freedoms."[193] The critical point is that nonspeech elements may create hazards for society above and beyond the speech elements. They are subject to regulation in appropriate circumstances because the government has an interest in dealing with the potential hazards of the nonspeech elements despite the fact that they are joined with expressive elements.

Thus, the starting point for analysis is whether the DMCA, as applied to restrict dissemination of DeCSS and other computer code used to circumvent access control measures, is a content based restriction on speech or a content neutral regulation. Put another way, the question is the level of review that governs the DMCA's anti-trafficking provision as applied to DeCSS—the strict scrutiny standard applicable to content based regulations or the intermediate level applicable to content neutral regulations, including regulations of the nonspeech elements of expressive conduct.

Given the fact that DeCSS code is expressive, defendants would have the Court leap immediately to the conclusion that Section 1201(a)(2)'s prohibition on providing DeCSS necessarily

---

192

During the Vietnam era, many who opposed the war, the draft, or both burned draft cards as acts of protest. Lower federal courts typically concluded or assumed that the expression inherent in this act of protest brought the behavior entirely within the scope of the First Amendment. THOMAS I. EMERSON, THE SYSTEM OF FREEDOM OF EXPRESSION 82 (1970). In *United States v. O'Brien*, 391 U.S. at 376, however, the Supreme Court rejected "the view that an apparently limitless variety of conduct can be labeled 'speech' whenever the person engaged in the conduct intends thereby to express an idea" and adopted a new approach, discussed below, to the regulation of expressive conduct as opposed to pure speech. *Accord, Spence v. State of Washington*, 418 U.S. 405, 410 (1974). The point for present purposes is that the presence of expression in some broader mosaic does not result in the entire mosaic being treated as "speech."

193

Id. at 376.

is content based regulation of speech because it suppresses dissemination of a particular kind of expression.[194] But this would be a unidimensional approach to a more textured reality and entirely too facile.

The "principal inquiry in determining content neutrality . . . is whether the government has adopted a regulation of speech because of [agreement or] disagreement with the message it conveys."[195] The computer code at issue in this case, however, does more than express the programmers' concepts. It does more, in other words, than convey a message. DeCSS, like any other computer program, is a series of instructions that causes a computer to perform a particular sequence of tasks which, in the aggregate, decrypt CSS-protected files. Thus, it has a distinctly functional, non-speech aspect in addition to reflecting the thoughts of the programmers. It enables anyone who receives it and who has a modicum of computer skills to circumvent plaintiffs' access control system.

The reason that Congress enacted the anti-trafficking provision of the DMCA had nothing to do with suppressing particular ideas of computer programmers and everything to do with functionality—with preventing people from circumventing technological access control measures—just as laws prohibiting the possession of burglar tools have nothing to do with preventing people from expressing themselves by accumulating what to them may be attractive assortments of implements and everything to do with preventing burglaries. Rather, it is focused squarely upon the

---

194 Def. Post-Trial Mem. at 15-16.

195 *Ward v. Rock Against Racism*, 491 U.S. 781, 791 (1989); *accord, Hill v. Colorado*, 120 S. Ct. 2480, 2491 (2000); *Turner Broadcasting System, Inc.*, 512 U.S. at 642; *Madsen v. Women's Health Center, Inc.*, 512 U.S. 753, 763 (1994).

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.[196]

These considerations suggest that the DMCA as applied here is content neutral, a view that draws support also from *City of Renton v. Playtime Theatres, Inc.*[197] The Supreme Court there upheld against a First Amendment challenge a zoning ordinance that prohibited adult movie theaters within 1,000 feet of a residential, church or park zone or within one mile of a school. Recognizing that the ordinance did "not appear to fit neatly into either the 'content based- or the 'content-neutral' category," it found dispositive the fact that the ordinance was justified without reference to the content of the regulated speech in that the concern of the municipality had been with the secondary effects of the presence of adult theaters, not with the particular content of the speech that takes place in them.[198] 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

---

196 *See generally Turner Broadcasting System, Inc.*, 512 U.S. at 646-49 (holding that "must-carry" provisions of the Cable Television Consumer Protection and Competition Act of 1992 are content neutral in view of "overriding congressional purpose . . . unrelated to the content of expression" manifest in detailed legislative history).

197 475 U.S. 41 (1986).

198 *Id.* at 46-49; *see also Young v. American Mini Theatres, Inc.*, 427 U.S. 50, 71 n.34 (1976).

neutral.[199]

Congress is not powerless to regulate content neutral regulations that incidentally affect expression, including the dissemination of the functional capabilities of computer code. A sufficiently important governmental interest in seeing to it that computers are not instructed to perform particular functions may justify incidental restrictions on the dissemination of the expressive elements of a program. Such a regulation will be upheld if:

> "it furthers an important or substantial governmental interest; if the governmental interest is unrelated to the suppression of free expression; and if the incidental restriction on alleged First Amendment freedoms is no greater than is essential to the furtherance of that interest."[200]

Moreover, "[t]o satisfy this standard, a regulation need not be the least speech-restrictive means of advancing the Government's interests."[201] "Rather, the requirement of narrow tailoring is satisfied 'so long as the . . . regulation promotes a substantial government interest that would be achieved less effectively absent the regulation.'"[202]

The anti-trafficking provision of the DMCA furthers an important governmental interest—the protection of copyrighted works stored on digital media from the vastly expanded risk of piracy in this electronic age. The substantiality of that interest is evident both from the fact that

---

199 *See Karn*, 925 F. Supp. at 10 (regulations controlling export of computer code content neutral); Benkler, 74 N.Y.U. L. REV. at 413 (DMCA "content and viewpoint neutral").

200 *Turner Broadcasting System, Inc.*, 512 U.S. at 662 (quoting *O'Brien*, 391 U.S. at 377 (internal quotation marks omitted)); *see also, e.g., United States v. Weslin*, 156 F.3d 292, 297 (2d Cir. 1998).

201 *Turner Broadcasting System, Inc.*, 512 U.S. at 662; *see also Hill*, 120 S. Ct. at 2494.

202 *Ward*, 491 U.S. at 799 (quoting *United States v. Albertini*, 472 U.S. 675, 689 (1985)).

the Constitution specifically empowers Congress to provide for copyright protection[203] and from the significance to our economy of trade in copyrighted materials.[204] Indeed, the Supreme Court has made clear that copyright protection itself is "the engine of free expression."[205] That substantial interest, moreover, is unrelated to the suppression of particular views expressed copyrighted works. Nor is the incidental restraint on protected expression—the prohibition of trafficking in means that would circumvent controls limiting access to unprotected materials or to copyrighted materials for noninfringing purposes—broader than is necessary to accomplish Congress' goals of preventing infringement and promoting the availability of content in digital form.[206]

This analysis finds substantial support in the principal case relied upon by defendants, *Junger v. Daley*.[207] The plaintiff in that case challenged on First Amendment grounds an Export Administration regulation that barred the export of computer encryption software, arguing that the software was expressive and that the regulation therefore was unconstitutional. The Sixth Circuit acknowledged the expressive nature of computer code, holding that it therefore was within the scope

---

203 U.S. CONST., art. I, § 8 (Copyright Clause).

204 COMMERCE COMM. REP. 94-95; SENATE REP. 21-22, 143.

205 *Harper & Row, Publishers, Inc. v. Nation Enterprises*, 471 U.S. 539, 558 (1985).

206 It is conceivable that technology eventually will provide means of limiting access only to copyrighted materials and only for uses that would infringe the rights of the copyright holder. *See, e.g.*, Travis, 15 BERKELEY TECH. L.J. at 835-36; Mark Gimbel, Note, Some Thoughts on the Implications of Trusted Systems for Intellectual Property Law, 50 Stan. L. Rev. 1671, 1875-78 (1998); Mark Stefik, *Shifting the Possible: How Trusted Systems and Digital Property Rights Challenge Us to Rethink Digital Publishing*, 12 BERKELEY TECH. L.J. 137, 138- 40 (1997). We have not yet come so far.

207 209 F.3d 481 (6th Cir. 2000).

of the First Amendment. But it recognized also that computer code is functional as well and said that "[t]he functional capabilities of source code, particularly those of encryption source code, should be considered when analyzing the governmental interest in regulating the exchange of this form of speech."[208] Indeed, it went on to indicate that the pertinent standard of review was that established in *United States v. O'Brien*,[209] the seminal speech-versus-conduct decision. Thus, rather than holding the challenged regulation unconstitutional on the theory that the expressive aspect of source code immunized it from regulation, the court remanded the case to the district court to determine whether the *O'Brien* standard was met in view of the functional aspect of code.[210]

Notwithstanding its adoption by the Sixth Circuit, the focus on functionality in order to determine the level of scrutiny is not an inevitable consequence of the speech-conduct distinction. Conduct has immediate effects on the environment. Computer code, on the other hand, no matter how functional, causes a computer to perform the intended operations only if someone uses the code to do so. Hence, one commentator, in a thoughtful article, has maintained that functionality is really "a proxy for effects or harm" and that its adoption as a determinant of the level of scrutiny slides over questions of causation that intervene between the dissemination of a computer program and any harm caused by its use.[211]

---

208 *Id.* at 485.

209 391 U.S. at 377.

210 209 F.3d at 485.

211 *See* Lee Tien, *Publishing Software as a Speech Act*, 15 BERKELEY TECH. L. J. 629, 694-701 (2000). Professor Tien's analysis itself has been criticized. Robert Post, *Encryption Source Code and the First Amendment*, 15 BERKELEY TECH. L. J. 715 (2000).

The characterization of functionality as a proxy for the consequences of use is accurate. But the assumption that the chain of causation is too attenuated to justify the use of functionality to determine the level of scrutiny, at least in this context, is not.

Society increasingly depends upon technological means of controlling access to digital files and systems, whether they are military computers, bank records, academic records, copyrighted works or something else entirely. There are far too many who, given any opportunity, will bypass those security measures, some for the sheer joy of doing it, some for innocuous reasons, and others for more malevolent purposes. Given the virtually instantaneous and worldwide dissemination widely available via the Internet, the only rational assumption is that once a computer program capable of bypassing such an access control system is disseminated, it will be used. And that is not all.

There was a time when copyright infringement could be dealt with quite adequately by focusing on the infringing act. If someone wished to make and sell high quality but unauthorized copies of a copyrighted book, for example, the infringer needed a printing press. The copyright holder, once aware of the appearance of infringing copies, usually was able to trace the copies up the chain of distribution, find and prosecute the infringer, and shut off the infringement at the source.

In principle, the digital world is very different. Once a decryption program like DeCSS is written, it quickly can be sent all over the world. Every recipient is capable not only of decrypting and perfectly copying plaintiffs' copyrighted DVDs, but also of retransmitting perfect copies of DeCSS and thus enabling every recipient to do the same. They likewise are capable of transmitting perfect copies of the decrypted DVD. The process potentially is exponential rather than linear. Indeed, the difference is illustrated by comparison of two epidemiological models describing

the spread of different kinds of disease.[212] In a common source epidemic, as where members of a population contract a non-contagious disease from a poisoned well, the disease spreads only by exposure to the common source. If one eliminates the source, or closes the contaminated well, the epidemic is stopped. In a propagated outbreak epidemic, on the other hand, the disease spreads from person to person. Hence, finding the initial source of infection accomplishes little, as the disease continues to spread even if the initial source is eliminated.[213] For obvious reasons, then, a propagated outbreak epidemic, all other things being equal, can be far more difficult to control.

This disease metaphor is helpful here. The book infringement hypothetical is analogous to a common source outbreak epidemic. Shut down the printing press (the poisoned well) and one ends the infringement (the disease outbreak). The spread of means of circumventing access to copyrighted works in digital form, however, is analogous to a propagated outbreak epidemic. Finding the original source of infection (e.g., the author of DeCSS or the first person to misuse it) accomplishes nothing, as the disease (infringement made possible by DeCSS and the resulting availability of decrypted DVDs) may continue to spread from one person who gains access to the circumvention program or decrypted DVD to another. And each is "infected," i.e., each is as capable of making perfect copies of the digital file containing the copyrighted work as the author of the

---

212 This perhaps is not as surprising as first might appear. Computer "viruses" are other programs, an understanding of which is aided by the biological analogy evident in their name. *See, e.g.*, Jeffrey O. Kephart, Gregory B. Sorkin, David M. Chess and Steve R. White, *Fighting Computer Viruses*, SCIENTIFIC AMERICAN, (visited Aug. 16, 2000) <http://www.sciam.com/1197issue/1197kephart.html>.

213 DAVID E. LILIENFELD & PAUL D. STOLLEY, FOUNDATIONS OF EPIDEMIOLOGY 38-41 & Fig. 3-1 (3d ed. 1994); JOHN P. FOX, CARRIE E. HALL & LILA R. ELVEBACK, EPIDEMIOLOGY—MAN AND DISEASE 246-47 (1970).

program or the first person to use it for improper purposes. The disease metaphor breaks down principally at the final point. Individuals infected with a real disease become sick, usually are driven by obvious self-interest to seek medical attention, and are cured of the disease if medical science is capable of doing so. Individuals infected with the "disease" of capability of circumventing measures controlling access to copyrighted works in digital form, however, do not suffer from having that ability. They cannot be relied upon to identify themselves to those seeking to control the "disease." And their self-interest will motivate some to misuse the capability, a misuse that, in practical terms, often will be untraceable.[214]

These considerations drastically alter consideration of the causal link between dissemination of computer programs such as this and their illicit use. Causation in the law ultimately involves practical policy judgments.[215] Here, dissemination itself carries very substantial risk of imminent harm because the mechanism is so unusual by which dissemination of means of circumventing access controls to copyrighted works threatens to produce virtually unstoppable infringement of copyright. In consequence, the causal link between the dissemination of circumvention computer programs and their improper use is more than sufficiently close to warrant selection of a level of constitutional scrutiny based on the programs' functionality.

---

214 Of course, not everyone who obtains DeCSS or some other decryption program necessarily will use it to engage in copyright infringement, just as not everyone who is exposed to a contagious disease contracts it. But that is immaterial. The critical point is that the combination of (a) the manner in which the ability to infringe is spread and (b) the lack of any practical means of controlling infringement at the point at which it occurs once the capability is broadly disseminated render control of infringement by controlling availability of the means of infringement far more critical in this context.

215 *See, e.g.*, Guido Calabresi & Jeffrey O. Cooper, *New Directions in Tort Law*, 30 VAL. U. L. REV. 859, 870-72 (1996).

Accordingly, this Court holds 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. In any case, its particular functional characteristics are such that the Court would apply the same level of scrutiny even if it were viewed as content based.[216] Yet it is important to emphasize that this is a very narrow holding. The restriction the Court here upholds, notwithstanding that computer code is within the area of First Amendment concern, is limited (1) to programs that circumvent access controls to copyrighted works in digital form in circumstances in which (2) there is no other practical means of preventing infringement through use of the programs, and (3) the regulation is motivated by a desire to prevent performance of the function for which the programs exist rather than any message they might convey. One readily might imagine other circumstances in which a governmental

---

216

As has been noted above, some categories of speech, which often have been referred to inaccurately as "unprotected," may be regulated on the basis of their content. *R.A.V.*, 505 U.S. at 382-83. These have included obscenity and "fighting words," to name two such categories. The determination of the types of speech which may be so regulated has been made through a process termed by one leading commentator as "definitional" balancing—a weighing of the value of free expression in these areas against its likely consequences and the legitimate interests of government. Melville B. Nimmer, *The Right to Speak from* Times *to* Time: *First Amendment Theory Applied to Libel and Misapplied to Privacy*, 56 CAL. L. REV. 935, 942 (1968); *see R.A.V.*, 505 U.S. at 382-83. Thus, even if one accepted defendants' argument that the anti-trafficking prohibition of the DMCA is content based because it regulates only code that "expresses" the programmer's "ideas" for circumventing access control measures, the question would remain whether such code—code designed to circumvent measures controlling access to private or legally protected data—nevertheless could be regulated on the basis of that content. For the reasons set forth in the text, the Court concludes that it may. Alternatively, even if such a categorical or definitional approach were eschewed, the Court would uphold the application of the DMCA now before it on the ground that this record establishes an imminent threat of danger flowing from dissemination of DeCSS that far outweighs the need for unfettered communication of that program. *See Landmark Communications, Inc. v. Virginia*, 435 U.S. 829, 842-43 (1978).

attempt to regulate the dissemination of computer code would not similarly be justified.[217]

2. Prior Restraint

Defendants argue also that injunctive relief against dissemination of DeCSS is barred by the prior restraint doctrine. The Court disagrees.

Few phrases are as firmly rooted in our constitutional jurisprudence as the maxim that "[a]ny system of prior restraints of expression comes to [a] Court bearing a heavy presumption against its constitutional validity."[218] Yet there is a significant gap between the rhetoric and the reality. Courts often have upheld restrictions on expression that many would describe as prior

---

217 For example, one might imagine a computer program the object of which was to teach the user a particular view of a subject, e.g., evolution or creationism. Such a program, like this one, would be within the area of First Amendment concern and functional. Yet a regulation barring its use would be subject to a quite different analysis. Such a ban, for example, might be based on the content of the message the program caused the computer to deliver to the student-user and thus quite clearly be content based. Similarly, the function—teaching—would not involve the same likelihood that the dissemination would bring about a harm that the government has a legitimate right to prevent.

218 *New York Times Co. v. United States*, 403 U.S. 713, 714 (1971) (per curiam) (quoting *Bantam Books, Inc. v. Sullivan*, 372 U.S. 58, 70 (1963)).

restraints,[219] sometimes by characterizing the expression as unprotected[220] and on other occasions finding the restraint justified despite its presumed invalidity.[221] Moreover, the prior restraint doctrine, which has expanded far beyond the Blackstonian model[222] that doubtless informed the understanding of the Framers of the First Amendment,[223] has been criticized as filled with "doctrinal ambiguities and inconsistencies result[ing] from the absence of any detailed judicial analysis of [its] true rationale"[224]

219

See, e.g., Posadas de Puerto Rico Assoc. v. Tourism Co. of Puerto Rico, 478 U.S. 328 (1986) (upholding restrictions on casino gambling advertising); *Times Film Corp. v. Chicago*, 365 U.S. 43 (1961) (upholding local ordinance requiring review of films by municipal officials as prerequisite to issuance of permits for public screening); *Salinger v. Random House, Inc.*, 811 F.2d 90 (2d Cir.) (enjoining biographer's use of subject's unpublished letters as copyright infringement), *cert. denied*, 484 U.S. 890 (1987); *Dallas Cowboys Cheerleaders v. Pussycat Cinema, Ltd.*, 604 F.2d 200 (2d Cir. 1979) (enjoining distribution of film on ground that actresses' uniforms infringed plaintiff's trademark). *See generally* LAURENCE H. TRIBE, AMERICAN CONSTITUTIONAL LAW § 12-36, at 1045-46 (1988) (hereinafter TRIBE).

220

See, e.g., Charles of the Ritz Group, Ltd. v. Quality King Distributors, Inc., 832 F.2d 1317 (2d Cir. 1987) (upholding injunction against commercial slogan on ground that slogan created a likelihood of confusion and is therefore "beyond the protective reach of the First Amendment"); *Vondran v. McLinn*, No. 95-20296, 1995 WL 415153, *6 (N.D. Cal. July 5, 1995) (enjoining defendant's false and disparaging remarks regarding plaintiff's patented process for making fiber reinforced concrete on the ground that the remarks are not protected by the First Amendment).

221

See, e.g., Times Film Corp., 365 U.S. 43 (upholding local ordinance requiring review by city officials of all films as a prerequisite to grant of permit for public screening despite concerns of First Amendment violations); *Posadas de Puerto Rico Assoc.*, 478 U.S. 328 (upholding restrictions on advertising despite finding that the advertising fell within ambit of First Amendment); *Dallas Cowboys Cheerleaders, Inc.*, 604 F.2d 200 (enjoining distribution of film for trademark infringement despite claim that injunction violated distributor's First Amendment rights).

222

4 WILLIAM BLACKSTONE, COMMENTARIES ON THE LAWS OF ENGLAND 151-52 (1769).

223

See Pittsburgh Press Co. v. Pittsburgh Comm. on Human Rel., 413 U.S. 376, 390 (1973).

224

Martin H. Redish, *The Proper Role of the Prior Restraint Doctrine in First Amendment Theory*, 70 VA. L. REV. 53, 54 (1983) (hereinafter "Redish"). *See also* LAURENCE H. TRIBE,

and, in one case, even as "fundamentally unintelligible."[225] Nevertheless, the doctrine has a well established core: administrative preclearance requirements for and at least preliminary injunctions against speech as conventionally understood are presumptively unconstitutional. Yet that proposition does not dispose of this case.[226]

The classic prior restraint cases were dramatically different from this one. *Near v. Minnesota*[227] involved a state procedure for abating scandalous and defamatory newspapers as public nuisances. *New York Times Co. v. United States*[228] dealt with an attempt to enjoin a newspaper from publishing an internal government history of the Vietnam War. *Nebraska Press Association v. Stuart*[229] concerned a court order barring the reporting of certain details about a forthcoming murder case. In each case, therefore, the government sought to suppress speech at the very heart of First Amendment concern—expression about public issues of the sort that is indispensable to self

---

AMERICAN CONSTITUTIONAL LAW § 12-34, at 1040-41 (2d ed. 1988).

225

John Calvin Jeffries, Jr., *Rethinking Prior Restraint*, 92 YALE L.J. 409, 419 (1983).

226

Despite the conventional wisdom, it is far from clear that an injunction necessarily is a prior restraint. Our circuit, for example, has suggested that the prior restraint doctrine does not apply to content neutral injunctions. *See e.g.*, *Dallas Cowboys Cheerleaders, Inc.*, 604 F.2d at 206. At least one commentator persuasively has argued that there is little justification for placing injunctions, at least permanent injunctions issued after trial, in a disfavored constitutional position. Jeffries, 92 YALE L.J. at 426-34. Nevertheless, there is no reason to decide that question in this case. The following discussion therefore assumes that the permanent injunction plaintiff seeks would be a "prior restraint," although it concludes that it would not be unconstitutional.

227

283 U.S. 697 (1931).

228

403 U.S. 713 (1971).

229

427 U.S. 539 (1976).

government. And while the prior restraint doctrine has been applied well beyond the sphere of political expression, we deal here with something new altogether—computer code, a fundamentally utilitarian construct, albeit one that embodies an expressive element. Hence, it would be a mistake simply to permit its expressive element to drive a characterization of the code as speech no different from the Pentagon Papers, the publication of a newspaper, or the exhibition of a motion picture and then to apply prior restraint rhetoric without a more nuanced consideration of the competing concerns.

In this case, the considerations supporting an injunction are very substantial indeed. Copyright and, more broadly, intellectual property piracy are endemic, as Congress repeatedly has found.[230] The interest served by prohibiting means that facilitate such piracy—the protection of the monopoly granted to copyright owners by the Copyright Act—is of constitutional dimension. There is little room for doubting that broad dissemination of DeCSS threatens ultimately to injure or destroy plaintiffs' ability to distribute their copyrighted products on DVDs and, for that matter, undermine

---

230 *See* H.R. REP. 106-216, 106th Cong., 1st Sess. (1999) ("Notwithstanding [penalties for copyright infringement] copyright piracy of intellectual property flourishes, assisted in large part by today's world of advanced technologies. For example, industry groups estimate that counterfeiting and piracy of computer software cost the affected copyright holders more than $11 billion last year (others believe the figure is closer to $20 billion). In some countries, software piracy rates are as high as 97% of all sales. The U.S. rate is far lower (25%), but the dollar losses ($2.9 billion) are the highest worldwide. The effect of this volume of theft is substantial: lost U.S. jobs, lost wages, lower tax revenue, and higher prices for honest purchasers of copyrighted software. Unfortunately, the potential for this problem to worsen is great."); S. REP. 106-140, 106th Cong., 1st Sess. (1999) ("Trademark owners are facing a new form of piracy on the Internet caused by acts of 'cybersquatting.'"); S. REP. 105-190, 105th Cong., 2d Sess. (1998) ("Due to the ease with which digital works can be copied and distributed worldwide virtually instantaneously, copyright owners will hesitate to make their works readily available on the Internet without reasonable assurance that they will be protected against massive piracy."); H.R. REP. 105-339, 105th Cong., 1st Sess. (1997) ("[C]opyright piracy flourishes in the software world.").

their ability to sell their products to the home video market in other forms. The potential damages probably are incalculable, and these defendants surely would be in no position to compensate plaintiffs for them if plaintiffs were remitted only to *post hoc* damage suits.

On the other side of the coin, the First Amendment interests served by the dissemination of DeCSS on the merits are minimal. The presence of some expressive content in the 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. Hence, those of the traditional rationales for the prior restraint doctrine that relate to inhibiting the transmission and receipt of ideas are of attenuated relevance here. Indeed, even academic commentators who take the extreme position that most injunctions in intellectual property cases are unconstitutional prior restraints concede that there is no First Amendment obstacle to injunctions barring distribution of copyrighted computer object code or restraining the construction of a new building based on copyrighted architectural drawings because the functional aspects of these types of information are "sufficiently nonexpressive."[231]

To be sure, there is much to be said in most circumstances for the usual procedural rationale for the prior restraint doctrine: prior restraints carry with them the risk of erroneously suppressing expression that could not constitutionally be punished after publication.[232] In this

---

231 Mark A. Lemley & Eugene Volokh, *Freedom of Speech and Injunctions in Intellectual Property Cases*, 48 DUKE L.J. 147, 210 & n.275 (1998).

232 *See, e.g.*, *Pittsburgh Press Co.*, 413 U.S. at 390 ("The special vice of a prior restraint is that communication will be suppressed . . . before an adequate determination that it is unprotected by the First Amendment."); Lemley & Volokh, 48 DUKE L.J. at 200-02, 211; *see* Redish, 70 VA. L. REV. at 75-83.

context, however, that concern is not persuasive, both because the enjoined expressive element is minimal and because a full trial on the merits has been held.[233] Accordingly, the Court holds that the prior restraint doctrine does not require denial of an injunction in this case.

3. Overbreadth

Defendants' second focus is the contention that Section 1201(a)(2) is unconstitutional because it prevents others from making fair use of copyrighted works by depriving them of the means of circumventing plaintiffs' access control system.[234] In substance, they contend that the anti-trafficking provision leaves those who lack sufficient technical expertise to circumvent CSS themselves without the means of acquiring circumvention technology that they need to make fair use of the content of plaintiffs' copyrighted DVDs.[235]

As a general proposition, "a person to whom a statute constitutionally may be applied may not challenge that statute on the ground that it conceivably may be applied unconstitutionally to

---

233 *See* Lemley & Volokh, 48 DUKE L.J. at 211-12, 215 (acknowledging that high likelihood of success diminishes risk of erroneous suppression of protected speech).

234 Def. Post-Trial Mem. at 22-24.

235 *Id.* at 22.

Defendants argue also that the DMCA as applied is overbroad in that "it would prohibit defendants from posting and making programs such as DeCSS available in any form, from English to any level of computer code." *Id.* The overbreadth doctrine, however, enables litigants to challenge a statute not merely because their own First Amendment rights are violated, but because the statute may cause others to abstain from constitutionally protected expression. *Broadrick v. Oklahoma*, 413 U.S. 601, 612 (1973). This aspect of defendants' argument, which in any case is an overstatement, therefore does not refer to overbreadth in the sense relevant here.

others in situations not before the Court."[236] When statutes regulate speech, however, "the transcendent value to all society of constitutionally protected expression is deemed to justify 'attacks on overly broad statutes with no requirement that the person making the attack demonstrate that his own conduct could not be regulated by a statute drawn with the requisite narrow specificity.'"[237] This is so because the absent third parties may not exercise their rights for fear of triggering "sanctions provided by a statute susceptible of application to protected expression."[238] But the overbreadth doctrine "'is 'strong medicine' . . . . employed . . . with hesitation, and then 'only as a last resort'" because it conflicts with "the personal nature of constitutional rights and the prudential limitations on constitutional adjudication," including the importance of focusing carefully on the facts in deciding constitutional questions.[239] Moreover, the limited function of the overbreadth doctrine "'attenuates as the otherwise unprotected behavior that it forbids the State to sanction moves from 'pure speech' toward conduct and that conduct—even if expressive—falls within the scope of otherwise valid criminal laws . . . .'"[240] As defendants concede, "where conduct and not merely speech is involved, . . . the overbreadth of a statute must not only be real, but substantial as well, judged in relation to

---

236 *Broadrick*, 413 U.S. at 610.

237 *Gooding v. Wilson*, 405 U.S. 518, 520-21 (1972) (quoting *Dombrowski v. Pfister*, 380 U.S. 479, 486 (1965)).

238 *Gooding*, 405 U.S. at 521.

239 *Los Angeles Police Department v. United Reporting Pub. Corp.*, 120 S. Ct. 483, 489 (1999) (quoting *New York v. Ferber*, 458 U.S. 747, 769 (1982) (quoting *Broadrick*, 413 U.S. at 613)).

240 *Id.* at 489 (quoting *Ferber*, 458 U.S. at 770 (quoting *Broadrick*, 413 U.S. at 615)).

the statute's plainly legitimate sweep."[241]

Factors arguing against use of the overbreadth doctrine are present here. To begin with, we do not here have a complete view of whether the interests of the absent third parties upon whom defendants rely really are substantial and, in consequence, whether the DMCA as applied here would materially affect their ability to make fair use of plaintiffs' copyrighted works.

The copyrighted works at issue, of course, are motion pictures. People use copies of them in DVD and other formats for various purposes, and we confine our consideration to the lawful purposes, which by definition are noninfringing or fair uses. The principal noninfringing use is to play the DVD for the purpose of watching the movie—viewing the images and hearing the sounds that are synchronized with them. Fair uses are much more varied. A movie reviewer might wish to quote a portion of the verbal script in an article or broadcast review. A television station might want to broadcast part of a particular scene to illustrate a review, a news story about a performer, or a story about particular trends in motion pictures. A musicologist perhaps would wish to play a portion of a musical sound track. A film scholar might desire to create and exhibit to students small segments of several different films to make some comparative point about the cinematography or some other characteristic. Numerous other examples doubtless could be imagined. But each necessarily involves one or more of three types of use: (1) quotation of the words of the script, (2) listening to the recorded sound track, including both verbal and non-verbal elements, and (3) viewing of the graphic images.

All three of these types of use now are affected by the anti-trafficking provision of the

---

[241] *Broadrick*, 413 U.S. at 612.

DMCA, but probably only to a trivial degree. To begin with, all or substantially all motion pictures available on DVD are available also on videotape.[242] In consequence, anyone wishing to make lawful use of a particular movie may buy or rent a videotape, play it, and even copy all or part of it with readily available equipment. But even if movies were available only on DVD, as someday may be the case, the impact on lawful use would be limited. Compliant DVD players permit one to view or listen to a DVD movie without circumventing CSS in any prohibited sense. The technology permitting manufacture of compliant DVD players is available to anyone on a royalty-free basis and at modest cost, so CSS raises no technological barrier to their manufacture. Hence, those wishing to make lawful use of copyrighted movies by viewing or listening to them are not hindered in doing so in any material way by the anti-trafficking provision of the DMCA.[243]

Nor does the DMCA materially affect quotation of language from CSS-protected movies. Anyone with access to a compliant DVD player may play the movie and write down or otherwise record the sound for the purpose of quoting it in another medium.

The DMCA does have a notable potential impact on uses that copy portions of a DVD

---

242 Tr. (King) at 441.

243 Defendants argue that the right of third parties to view DVD movies on computers running the Linux operating system will be materially impaired if DeCSS is not available to them. However, the technology to build a Linux-based DVD player has been licensed by the DVD CCA to at least two companies, and there is no reason to think that others wishing to develop Linux players could not obtain licenses if they so chose. Tr. (King) at 437-38. Therefore, enforcement of the DMCA to prohibit the posting of DeCSS would not materially impair the ability of Linux users to view DVDs on Linux machines. Further, it is not evident that constitutional protection of free expression extends to the type of device on which one plays copyrighted material. Therefore, even assuming *arguendo* that the ability of third parties to view DVD movies on Linux systems were materially impaired by enforcement of the DMCA in this case, this impairment would not necessarily implicate the First Amendment rights of these third parties.

movie because compliant DVD players are designed so as to prevent copying. In consequence, even though the fair use doctrine permits limited copying of copyrighted works in appropriate circumstances, the CSS encryption of DVD movies, coupled with the characteristics of licensed DVD players, limits such uses absent circumvention of CSS.[244] Moreover, 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.[245]

As the foregoing suggests, the interests of persons wishing to circumvent CSS in order to make lawful use of the copyrighted movies it protects are remarkably varied. Some presumably are technologically sophisticated and therefore capable of circumventing CSS without access to defendants' or other purveyors' decryption programs; many presumably are not. Many of the possible fair uses may be made without circumventing CSS while others, i.e., those requiring copying,

---

244 CSS encryption coupled with the characteristics of compliant DVD players also forecloses copying of digital sound files. It is not clear, however, that this is a substantial impediment to copying sound from motion picture DVDs. A DVD can be played on a compliant player and the sound re-recorded. Whether the sound quality thus obtained would be satisfactory might well depend upon the particular use to which the copy was put.

245 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.

may not. Hence, the question whether Section 1201(a)(2) as applied here substantially affects rights, much less constitutionally protected rights, of members of the "fair use community" cannot be decided *in bloc*, without consideration of the circumstances of each member or similarly situated groups of members. Thus, the prudential concern with ensuring that constitutional questions be decided only when the facts before the Court so require counsels against permitting defendants to mount an overbreadth challenge here.[246]

Second, there is no reason to suppose here that prospective fair users will be deterred from asserting their alleged rights by fear of sanctions imposed by the DMCA or the Copyright Act.

Third, we do not deal here with "pure speech." Rather, the issue concerns dissemination of technology that is principally functional in nature. The same consideration that warrants restraint in applying the overbreadth doctrine to statutes regulating expressive conduct applies here. For reasons previously expressed, government's interest in regulating the functional capabilities of computer code is no less weighty than its interest in regulating the nonspeech aspects of expressive conduct.

Finally, there has been no persuasive evidence that the interests of persons who wish access to the CSS algorithm in order to study its encryption methodology or to evaluate theories regarding decryption raise serious problems. The statute contains an exception for good faith

---

246

Defendants argue that "there is now a full evidentiary record" and that the overbreadth issue therefore should be decided. Def. Post-Trial Mem. at 22 n.11. With respect, the evidence as to the impact of the anti-trafficking provision of the DMCA on prospective fair users is scanty and fails adequately to address the issues.

This is not to minimize the interests of the *amici* who have submitted briefs in this case. The Court simply does not have a sufficient evidentiary record on which to evaluate their claims.

encryption research.[247]

Accordingly, defendants will not be heard to mount an overbreadth challenge to the DMCA in this context.

4. Vagueness

Defendants argue also that the DMCA is unconstitutionally vague because the terms it employs are not understandable to persons of ordinary intelligence and because they are subject to discriminatory enforcement.[248]

As the Supreme Court has made clear, one who "engages in some conduct that is clearly proscribed [by the challenged statute] cannot complain of the vagueness of the law as applied to the conduct of others."[249] There can be no serious doubt that posting a computer program the sole purpose of which is to defeat an encryption system controlling access to plaintiff's copyrighted movies constituted an "offer to the public" of "technology [or a] product" that was "primarily designed for the purpose of circumventing" plaintiffs' access control system.[250] Defendants thus engaged in conduct clearly proscribed by the DMCA and will not be heard to complain of any vagueness as applied to others.

---

247 17 U.S.C. § 1201(g).

248 Def. Post-Trial Mem. at 24.

249 *Village of Hoffman Estates v. Flipside*, 455 U.S. 489, 495 (1982).

250 *See* 17 U.S.C. § 1201(a)(2)(A).

C. Linking

As indicated above, the DMCA reaches links deliberately created by a web site operator for the purpose of disseminating technology that enables the user to circumvent access controls on copyrighted works. The question is whether it may do so consistent with the First Amendment.

Links bear a relationship to the information superhighway comparable to the relationship that roadway signs bear to roads but they are more functional. Like roadway signs, they point out the direction. Unlike roadway signs, they take one almost instantaneously to the desired destination with the mere click of an electronic mouse. Thus, like computer code in general, they have both expressive and functional elements. Also like computer code, they are within the area of First Amendment concern. Hence, the constitutionality of the DMCA as applied to defendants' linking is determined by the same *O'Brien* standard that governs trafficking in the circumvention technology generally.

There is little question that the application of the DMCA to the linking at issue in this case would serve, at least to some extent, the same substantial governmental interest as its application to defendants' posting of the DeCSS code. Defendants' posting and their linking amount to very much the same thing. Similarly, the regulation of the linking at issue here is "unrelated to the suppression of free expression" for the same reason as the regulation of the posting. The third prong of the *O'Brien* test as subsequently interpreted—whether the "regulation promotes a substantial government interest that would be achieved less effectively absent the regulation"[251]—is a somewhat

---

[251] *Ward*, 491 U.S. at 799 (quoting *United States v. Albertini*, 472 U.S. 675, 689 (1985)).

closer call.

Defendants and, by logical extension, others may be enjoined from posting DeCSS. Plaintiffs may seek legal redress against anyone who persists in posting notwithstanding this decision. Hence, barring defendants from linking to sites against which plaintiffs readily may take legal action would advance the statutory purpose of preventing dissemination of circumvention technology, but it would do so less effectively than would actions by plaintiffs directly against the sites that post. For precisely this reason, however, the real significance of an anti-linking injunction would not be with U.S. web sites subject to the DMCA, but with foreign sites that arguably are not subject to it and not subject to suit here. An anti-linking injunction to that extent would have a significant impact and thus materially advance a substantial governmental purpose. In consequence, the Court concludes that an injunction against linking to other sites posting DeCSS satisfies the *O'Brien* standard. There remains, however, one further important point.

Links are "what unify the [World Wide] Web into a single body of knowledge, and what makes the Web unique."[252] They "are the mainstay of the Internet and indispensable to its convenient access to the vast world of information."[253] They often are used in ways that do a great deal to promote the free exchange of ideas and information that is a central value of our nation. Anything that would impose strict liability on a web site operator for the entire contents of any web site to which the operator linked therefore would raise grave constitutional concerns, as web site

---

[252] *ACLU v. Reno*, 929 F. Supp. 824, 837 (E.D. Pa. 1996), *aff'd*, 521 U.S. 844 (1997).

[253] Richard Raysman & Peter Brown, *Recent Linking Issues*, N.Y.L.J., Feb. 8, 2000, p. 3, col. 1.

operators would be inhibited from linking for fear of exposure to liability.[254] And it is equally clear that exposing those who use links to liability under the DMCA might chill their use, as some web site operators confronted with claims that they have posted circumvention technology falling within the statute may be more inclined to remove the allegedly offending link rather than test the issue in court. Moreover, web sites often contain a great variety of things, and a ban on linking to a site that contains DeCSS amidst other content threatens to restrict communication of this information to an excessive degree.

The possible chilling effect of a rule permitting liability for or injunctions against Internet hyperlinks is a genuine concern. But it is not unique to the issue of linking. The constitutional law of defamation provides a highly relevant analogy. The threat of defamation suits creates the same risk of self-censorship, the same chilling effect, for the traditional press as a prohibition of linking to sites containing circumvention technology poses for web site operators. Just as the potential chilling effect of defamation suits has not utterly immunized the press from all actions for defamation, however, the potential chilling effect of DMCA liability cannot utterly immunize web site operators from all actions for disseminating circumvention technology. And the solution to the problem is the same: the adoption of a standard of culpability sufficiently high to immunize the activity, whether it is publishing a newspaper or linking, except in cases in which the conduct in question has little or no redeeming constitutional value.

In the defamation area, this has been accomplished by a two-tiered constitutional standard. There may be no liability under the First Amendment for defamation of a public official or

---

[254] *Cf. New York Times Co. v. Sullivan*, 376 U.S. 254, 271-73, 283-88 (1964).

a public figure unless the plaintiff proves, by clear and convincing evidence, that the defendant published the offending statement with knowledge of its falsity or with serious doubt as to its truth.[255] Liability in private figure cases, on the other hand, may not be imposed absent proof at least of negligence under *Gertz v. Robert Welch, Inc.*[256] A similar approach would minimize any chilling effect here.

The other concern—that a liability based on a link to another site simply because the other site happened to contain DeCSS or some other circumvention technology in the midst of other perfectly appropriate content could be overkill—also is readily dealt with. The offense under the DMCA is offering, providing or otherwise trafficking in circumvention technology. An essential ingredient, as explained above, is a desire to bring about the dissemination. Hence, a strong requirement of that forbidden purpose is an essential prerequisite to any liability for linking.

Accordingly, there may be no injunction against, nor liability for, linking to a site containing circumvention technology, the offering of which is unlawful under the DMCA, absent 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.[257] Such a standard will limit the fear of liability on the part of web site operators just as

---

255 *Id.* at 283; *Curtis Pub. Co. v. Butts*, 388 U.S. 130, 155 (1967); *St. Amant v. Thompson*, 390 U.S. 727, 731 (1968); ROBERT D. SACK, SACK ON DEFAMATION § 1.2.4 (3d ed. 1999).

256 418 U.S. 323, 347-38 (1974).

257 In evaluating purpose, courts will look at all relevant circumstances. Sites that advertise their links as means of getting DeCSS presumably will be found to have created the links for the purpose of disseminating the program. Similarly, a site that deep links to a page containing

the *New York Times* standard gives the press great comfort in publishing all sorts of material that would have been actionable at common law, even in the face of flat denials by the subjects of their stories. And it will not subject web site operators to liability for linking to a site containing proscribed technology where the link exists for purposes other than dissemination of that technology.

In this case, plaintiffs have established by clear and convincing evidence that these defendants linked to sites posting DeCSS, knowing that it was a circumvention device. Indeed, they initially touted it as a way to get free movies,[258] and they later maintained the links to promote the dissemination of the program in an effort to defeat effective judicial relief. They now know that dissemination of DeCSS violates the DMCA. An anti-linking injunction on these facts does no violence to the First Amendment. Nor should it chill the activities of web site operators dealing with different materials, as they may be held liable only on a compelling showing of deliberate evasion of the statute.

IV. Relief

A. Injury to Plaintiffs

The DMCA provides that "[a]ny person injured by a violation of section 1201 or 1202 may bring a civil action in an appropriate United States court for such violation."[259] For the reasons

---

only DeCSS located on a site that contains a broad range of other content, all other things being equal, would more likely be found to have linked for the purpose of disseminating DeCSS than if it merely links to the home page of the linked-to site.

258 Tr. (Corley) at 820.

259 17 U.S.C. § 1203(a).

set forth above, plaintiffs obviously have suffered and, absent effective relief, will continue to suffer injury by virtue of the ready availability of means of circumventing the CSS access control system on their DVDs. Defendants nevertheless argue that they have not met the injury requirement of the statute. Their contentions are a farrago of distortions.

They begin with the assertion that plaintiffs have failed to prove that decrypted motion pictures actually are available.[260] To be sure, plaintiffs might have done a better job of proving what appears to be reasonably obvious. They certainly could have followed up on more of the 650 movie titles listed on the web site described above to establish that the titles in fact were available. But the evidence they did adduce is not nearly as meager as defendants would have it. Dr. Shamos did pursue and obtain a pirated copy of a copyrighted, DivX'd motion picture from someone he met in an Internet chat room. An MPAA investigator downloaded between five and ten such copies. And the sudden appearance of listings of available motion pictures on the Internet promptly after DeCSS became available is far from lacking in evidentiary significance. In any case, in order to obtain the relief sought here, plaintiffs need show only a threat of injury by reason of a violation of the statute.[261] The Court finds that plaintiffs overwhelmingly have established a clear threat of injury by reason of defendants' violation of the statute.

Defendants next maintain that plaintiffs exaggerate the extent of the threatened injury. They claim that the studios in fact believe that DeCSS is not a threat.[262] But the only basis for that

---

260 Def. Post-Trial Mem. at 27-28.

261 The statute expressly authorizes injunctions to prevent or restrain violations, 17 U.S.C. § 1203(b)(1), thus demonstrating that the requisite injury need only be threatened.

262 Def. Post-Trial Mem. at 28.

contention is a couple of quotations from statements that the MPAA or one or another studio made (or considered making but did not in fact issue) to the effect that it was not concerned about DeCSS or that it was inconvenient to use.[263] These statements, however, were attempts to "spin" public opinion.[264] They do not now reflect the actual state of affairs or the studios' actual views, if they ever did.

Third, defendants contend that there is no evidence that any decrypted movies that may be available, if any there are, were decrypted with DeCSS. They maintain that "[m]any utilities and devices . . . can decrypt DVDs equally well and often faster and with greater ease than by using DeCSS."[265] This is a substantial exaggeration. There appear to be a few other so-called rippers, but the Court finds that DeCSS is usable on a broader range of DVDs than any of the others. Further, there is no credible evidence that any other utility is faster or easier to use than DeCSS. Indeed, the Court concludes that DeCSS is the superior product, as evidenced by the fact that the web site promoting DivX as a tool for obtaining usable copies of copyrighted movies recommends the use of DeCSS, rather than anything else, for the decryption step[266] and that the apparent availability of pirated motion pictures shot up so dramatically upon the introduction of DeCSS.[267]

---

263 *Id.* at 28-29.

264 *See, e.g.*, Ex. AYZ (Hunt Dep.) at 94-104.

265 *Id.* 30.

266 Ex. 113.

267 Defendants' argument would lack merit even if there were credible proof that other circumvention devices actually exist and produce results comparable to DeCSS. The available movies must have been decrypted with DeCSS or something else. As far as this

B. Permanent Injunction and Declaratory Relief

Plaintiffs seek a permanent injunction barring defendants from posting DeCSS on their web site and from linking their site to others that make DeCSS available.

The starting point, as always, is the statute. The DMCA provides in relevant part that the court in an action brought pursuant to its terms "may grant temporary and permanent injunctions on such terms as it deems reasonable to prevent or restrain a violation . . . ."[268] Where statutes in substance so provide, injunctive relief is appropriate if there is a reasonable likelihood of future violations absent such relief[269] and, in cases brought by private plaintiffs, if the plaintiff lacks an

---

record discloses, any such device or technology would violate the DMCA for the same reasons as does DeCSS. In consequence, this case comes within the principle of *Summers v. Tice*, 33 Cal. 2d 80, 199 P.2d 1 (1948). Where, as here, two or more persons take substantially identical wrongful actions, one and only one of which had to be the source of the plaintiffs' injury, and it is equally likely that one inflicted the injury as the other, the burden of proof on causation shifts to the defendants, each of which is liable absent proof that its action did not cause the injury. *See* 4 Fowler V. Harper & Fleming James, Jr., THE LAW OF TORTS §§ 101-04 (2d ed. 1996).

Defendants' efforts to avoid the consequences of this common sense principle are unpersuasive. They argue, for example, that plaintiffs may not invoke the theory unless they join as defendants everyone who may have contributed to the injury. Def. Post-Trial Mem. at 32 n.18 (citing Ex. UZ). It would be difficult to imagine a more nonsensical requirement in the context of this case. Where, as here, harm is done by dissemination of information over the Internet, probably by a substantial number of people all over the world, defendants' proposed rule would foreclose judicial relief anywhere because joinder of all plainly would be impossible in any one place, and technology does not permit identification of which wrongdoer's posting or product led to which pirated copy of a copyrighted work.

268 17 U.S.C. § 1203(b)(1).

269 *See, e.g., SEC v. Unique Financial Concepts, Inc.*, 196 F.3d 1195, 1199 n.2 (2d Cir. 1999) (injunction under Section 20(b) of the Securities Act of 1933, 15 U.S.C. § 77t(b), which permits an injunction "upon a proper showing," requires "a reasonable likelihood that the wrong will be repeated"); *CFTC v. Hunt*, 591 F.2d 1211, 1220 (7th Cir. 1979) (same under Commodity Exchange Act, 7 U.S.C. § 13a-1(b)); *SEC v. Bausch & Lomb Inc.*, 577 F.2d 8,

adequate remedy at law.[270]

In this case, it is quite likely that defendants, unless enjoined, will continue to violate the Act. Defendants are in the business of disseminating information to assist hackers in "cracking" various types of technological security systems. And while defendants argue that they promptly stopped posting DeCSS when enjoined preliminarily from doing so, thus allegedly demonstrating their willingness to comply with the law, their reaction to the preliminary injunction in fact cuts the other way. Upon being enjoined from posting DeCSS themselves, defendants encouraged others to "mirror" the information—that is, to post DeCSS—and linked their own web site to mirror sites in order to assist users of defendants' web site in obtaining DeCSS despite the injunction barring defendants from providing it directly. While there is no claim that this activity violated the letter of the preliminary injunction, and it therefore presumably was not contumacious, and while its status under the DMCA was somewhat uncertain, it was a studied effort to defeat the purpose of the preliminary injunction. In consequence, the Court finds that there is a substantial likelihood of future violations absent injunctive relief.

There also is little doubt that plaintiffs have no adequate remedy at law. The only potential legal remedy would be an action for damages under Section 1203(c), which provides for recovery of actual damages or, upon the election of the plaintiff, statutory damages of up to $2,500

---

18 (2d Cir. 1977) (reasonable likelihood of future violations required under § 21(d) of Securities Exchange Act of 1934, 15 U.S.C. § 78u(d), which permits an injunction "upon a proper showing" where person "engaged or . . . about to engage in" violation of statute).

270 *See, e.g.*, *Rondeau v. Mosinee Paper Corp.*, 422 U.S. 49, 57 (1975) (injunctive relief in private action under § 13(d) of the Securities Exchange Act of 1934, 15 U.S.C. § 78m(d), as added by the Williams Act, requires a showing of irreparable harm and inadequacy of legal remedies).

per offer of DeCSS. Proof of actual damages in a case of this nature would be difficult if not virtually impossible, as it would involve proof of the extent to which motion picture attendance, sales of broadcast and other motion picture rights, and sales and rentals of DVDs and video tapes of movies were and will be impacted by the availability of DVD decryption technology. Difficulties in determining what constitutes an "offer" of DeCSS in a world in which the code is available to much of the world via Internet postings, among other problems, render statutory damages an inadequate means of redressing plaintiffs' claimed injuries. Indeed, difficulties such as this have led to the presumption that copyright and trademark infringement cause irreparable injury,[271] i.e., injury for which damages are not an adequate remedy.[272] The Court therefore holds that the traditional requirements for issuance of a permanent injunction have been satisfied. Yet there remains another point for consideration.

Defendants argue that an injunction in this case would be futile because DeCSS already is all over the Internet. They say an injunction would be comparable to locking the barn door after the horse is gone. And the Court has been troubled by that possibility. But the countervailing arguments overcome that concern.

To begin with, any such conclusion effectively would create all the wrong incentives

---

271 *Tough Traveler, Ltd. v. Outbound Prods.*, 60 F.3d 964, 967-68 (2d Cir. 1995) (trademark); *Fisher-Price, Inc. v. Well-Made Toy Mfg. Corp.*, 25 F.3d 119, 124 (2d Cir. 1994) (copyright).

272 *See, e.g.*, *Northwestern Nat'l Ins. Co. v. Alberts*, 937 F.2d 77, 80 (2d Cir. 1991) ("The irreparable injury requisite . . . overlaps with the absent lack of adequate remedy at law necessary to establish the equitable rights."); *Buffalo Forge Co. v. Ampco-Pittsburgh Corp.*, 638 F.2d 568, 569 (2d Cir. 1981) ("There must also be a showing of irreparable harm, the absence of an adequate remedy at law, which is the *sine qua non* for the grant of such equitable relief.")

by allowing defendants to continue violating the DMCA simply because others, many doubtless at defendants' urging, are doing so as well. Were that the law, defendants confronted with the possibility of injunctive relief would be well advised to ensure that others engage in the same unlawful conduct in order to set up the argument that an injunction against the defendants would be futile because everyone else is doing the same thing.

Second, and closely related, is the fact that this Court is sorely "troubled by the notion that any Internet user . . . can destroy valuable intellectual property rights by posting them over the Internet."[273] While equity surely should not act where the controversy has become moot, it ought to look very skeptically at claims that the defendant or others already have done all the harm that might be done before the injunction issues.

The key to reconciling these views is that the focus of injunctive relief is on the defendants before the Court. If a plaintiff seeks to enjoin a defendant from burning a pasture, it is no answer that there is a wild fire burning in its direction. If the defendant itself threatens the plaintiff with irreparable harm, then equity will enjoin the defendant from carrying out the threat even if other threats abound and even if part of the pasture already is burned.

These defendants would harm plaintiffs every day on which they post DeCSS on their heavily trafficked web site and link to other sites that post it because someone who does not have DeCSS thereby might obtain it. They thus threaten plaintiffs with immediate and irreparable injury. They will not be allowed to continue to do so simply because others may do so as well. In short, this Court, like others than have faced the issued, is "not persuaded that modern technology has withered

---

[273] *Religious Tech. Ctr. v. Netcom On-Line Comm. Servs., Inc.*, 923 F. Supp. 1231, 1256 (N.D. Cal. 1995).

the strong right arm of equity."[274] Indeed, the likelihood is that this decision will serve notice on others that "the strong right arm of equity" may be brought to bear against them absent a change in their conduct and thus contribute to a climate of appropriate respect for intellectual property rights in an age in which the excitement of ready access to untold quantities of information has blurred in some minds the fact that taking what is not yours and not freely offered to you is stealing. Appropriate injunctive[275] and declaratory relief will issue simultaneously with this opinion.

V. Miscellaneous Contentions

There remain for consideration two other matters, plaintiffs' application for costs and attorney's fees and defendants' pretrial complaints concerning discovery.

The DMCA permits awards of costs and attorney's fees to the prevailing party in the discretion of the Court.[276] Insofar as attorney's fees are concerned, this is an exception to the so-

---

274 *Com-Share, Inc. v. Computer Complex, Inc.*, 338 F. Supp. 1229, 1239 (E.D. Mich. 1971).

275 During the trial, Professor Touretzky of Carnegie Mellon University, as noted above, convincingly demonstrated that computer source and object code convey the same ideas as various other modes of expression, including spoken language descriptions of the algorithm embodied in the code. Tr. (Touretzky) at 1068-69; Ex. BBE, CCO, CCP, CCQ. He drew from this the conclusion that the preliminary injunction irrationally distinguished between the code, which was enjoined, and other modes of expression that convey the same idea, which were not, *id.*, although of course he had no reason to be aware that the injunction drew that line only because that was the limit of the relief plaintiffs sought. With commendable candor, he readily admitted that the implication of his view that the spoken language and computer code versions were substantially similar was not necessarily that the preliminary injunction was too broad; rather, the logic of his position was that it was either too broad *or* too narrow. *Id.* at 1070-71. Once again, the question of a substantially broader injunction need not be addressed here, as plaintiffs have not sought broader relief.

276 17 U.S.C. § 1203(b)(4)-(b)(5).

called "American rule" pursuant to which each side in a litigation customarily bears its own attorney's fees. As this was a test case raising important issues, it would be inappropriate to award attorney's fees pursuant to the DMCA.[277] There is no comparable reason, however, for failing to award costs, particularly as taxable costs are related to the excessive discovery demands that the Court already has commented upon.[278]

A final word is in order in view of defendants' repeated pretrial claims that their discovery efforts were being thwarted. During the course of the trial, they applied for leave to take one deposition, which was granted. At no point did they make any showing that they were hampered in presenting their case or meeting the plaintiffs' case by virtue of any failure to obtain discovery. They applied for no continuance. They have not sought a new trial. And though they estimated that their case would take several weeks to present, the entire trial was completed in six days. Indeed, in the Court's view, the trial fully vindicated its pretrial assessment that there were, in actuality, very few genuinely disputed questions of material fact, and most of those involved expert testimony that was readily available to both sides.[279] Examination of the trial record will reveal that virtually the entire case could have been stipulated, although the legal conclusions to be drawn from the stipulated facts of course would have remained a matter of controversy.

---

277 *See Fogerty v. Fantasy, Inc.*, 510 U.S. 517, 534 (1994) (articulating factors relevant to fee awards under the Copyright Act).

278 *Universal City Studios, Inc. v. Reimerdes*, 00 Civ. 0277 (LAK), 2000 WL 987285 (S.D.N.Y. July 17, 2000).

279 The chief factual issue actually litigated at trial was the speed with which decrypted files could be transmitted over the Internet and other networks.

VI. Conclusion

In the final analysis, the dispute between these parties is simply put if not necessarily simply resolved.

Plaintiffs have invested huge sums over the years in producing motion pictures in reliance upon a legal framework that, through the law of copyright, has ensured that they will have the exclusive right to copy and distribute those motion pictures for economic gain. They contend that the advent of new technology should not alter this long established structure.

Defendants, on the other hand, are adherents of a movement that believes that information should be available without charge to anyone clever enough to break into the computer systems or data storage media in which it is located. Less radically, they have raised a legitimate concern about the possible impact on traditional fair use of access control measures in the digital era.

Each side is entitled to its views. In our society, however, clashes of competing interests like this are resolved by Congress. For now, at least, Congress has resolved this clash in the DMCA and in plaintiffs' favor. Given the peculiar characteristics of computer programs for circumventing encryption and other access control measures, the DMCA as applied to posting and linking here does not contravene the First Amendment. Accordingly, plaintiffs are entitled to appropriate injunctive and declaratory relief.

SO ORDERED.

Dated: August 17, 2000

Lewis A. Kaplan
United States District Judge