**UNIVERSAL CITY STUDIOS, INC, et al., v. REIMERDES, et al.,**

**UNITED STATES DISTRICT COURT FOR THE SOUTHERN DISTRICT OF NEW YORK**

***111 F. Supp. 2d 294* *2000***

**August 17, 2000, Decided**

**August 17, 2000, Filed**

*\*\*\*\*\*\**

*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 . . . . consisting 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. "More 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 **[\*\*7]** 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 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*

"Computers 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) 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 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 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 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 1/2 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 **[\*\*15]** and digital versatile disks, or DVDs.

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

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 unlicensed players and make digital copies of DVD movies. 30 The quality of motion pictures decrypted by DeCSS is virtually identical to that of encrypted movies on DVD. 31

*\*\*\**

*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 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 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

*\*\*\**

*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

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.

The DMCA contains two principal anticircumvention provisions. The first, *Section 1201(a)(1)*, governs "the 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 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 of the statute. 135 "Circumvent 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.

*\*\*\**

*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. … 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 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, 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*. But that conclusion still 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.

In general, "government has no power to restrict expression because of its message, its ideas, its subject matter, or its content . . . ." 187 "Subject 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 Even if conduct contains an expressive element, its nonspeech aspect need not be ignored. 192 "When '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 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 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 neutral.

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, "to 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 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 in means of gaining access to protected 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 of the *First Amendment*. But it recognized also that computer code is functional as well and said that "the 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

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 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.

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 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 "any 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 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 resulting from the absence of any detailed judicial analysis of [its] true rationale" 224 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 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 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

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

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 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.

\*\*\*

*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 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 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 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 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.

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 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.

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.

\*\*\*

*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.