

2000 U.S. Dist. LEXIS 11696, *; 55 U.S.P.Q.2D (BNA) 1873;
Copy. L. Rep. (CCH) P28,122

[note: edited version]

**UNIVERSAL CITY STUDIOS, INC, et al., Plaintiffs, -against- SHAWN C.
REIMERDES, et al., Defendants.**

00 Civ. 0277 (LAK)

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

*2000 U.S. Dist. LEXIS 11696; 55 U.S.P.Q.2D (BNA) 1873; Copy. L. Rep. (CCH)
P28,122*

August 17, 2000, Decided

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 [*2] 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") n1 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.

n1 *17 U.S.C. § 1201 et seq.*

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. n2 This is the Court's decision after trial, and the decision may be summarized in a nutshell.

[*3]

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 anticircumvention measures would [*4] 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. n3 But the solution it enacted is clear. The potential tension to which defendants point does not absolve them of liability under the statute. There is no serious question that defendants' posting of DeCSS violates the DMCA.

* * *

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. n27 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. n28 The technology necessary to configure DVD players and drives to play CSS-protected DVDs n29 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. n30 The quality of motion pictures decrypted by DeCSS is virtually identical to that of encrypted movies [*17] on DVD. n31

DivX is a compression program available for download over the Internet. n32 It compresses video files in order to minimize required storage space, often to facilitate transfer over the Internet or other networks. n33

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. n34 Plaintiffs produce and distribute a large majority of the motion pictures on DVDs on the market today. n35

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*. n36 He and his company, defendant 2600 Enterprises, Inc., together publish a magazine called *2600: The Hacker Quarterly*, which Corley founded in 1984, n37 and which is something of a bible to the hacker community. n38 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. n39 Mr. Corley chose the name because he regarded it as a "mystical thing," n40 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, n41 access other people's e-mail, n42 intercept cellular phone

calls, n43 and break into the computer systems at Costco stores n44 and Federal Express. n45 One issue contains a guide to the federal criminal justice system for readers charged [*19] with computer hacking. n46 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. n47

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. n48 At that time, 2600.com contained also a list of links to other web sites purporting to post DeCSS. n49

* * *

[T]he technology for making compliant devices, i.e., devices with CSS keys, had to be licensed to consumer electronics manufacturers. n60 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 [*24] is licensed subject to strict security requirements. n61 Moreover, manufacturers may not, consistent with their licenses, make equipment that would supply digital output that could be used in copying protected DVDs. n62 Licenses to manufacture compliant devices are granted on a royalty-free basis subject only to an administrative fee. n63 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. n64

* * *

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. n71 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 drives. n72 Mr. Johansen then [*27] posted the executable code on his personal Internet web site and informed members of an Internet mailing list that he had done so. n73 Neither Mr. Johansen nor his collaborators obtained a license from the DVD CCA. n74

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, n75 DeCSS is a Windows executable file; that is, it can be executed only on computers running the Windows operating system. n76 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 [*28] the file system used on DVDs. n77 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. n78 Assuming that to be true, n79 however, 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. n80 The disposition of the Norwegian [*29] 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. n81 A few other applications said to decrypt CSS-encrypted DVDs also have appeared on the Internet. n82

In November 1999, defendants' web site began to offer DeCSS for download. n83 It established also a list of links to several web sites that purportedly "mirrored" or offered DeCSS for download. n84 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. n85 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. n86 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. n87 Finally, the user may be brought directly to the DeCSS link on the linked-to site such that download of DeCSS begins immediately

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 October 1999. n89 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. n90 In January 2000, the studios filed this lawsuit against [*32] defendant Eric Corley and two others. n91

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. n92 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. n93

Following the issuance of the preliminary injunction, defendants removed DeCSS from the 2600.com web site. n94 In what they termed an act of "electronic civil disobedience," n95 however, they continued to support links to other web sites purporting to offer DeCSS for download, a list which had grown to nearly five hundred by July 2000. n96 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." n97

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 [*34] 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. n98

* * *

II. The Digital Millennium Copyright Act

A. . . .

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." n131 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." n132 As defendants are accused here only of posting and linking to [*46] 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.

B. Posting of DeCSS

1. Violation of Anti-Trafficking [*47] 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]."

In this case, defendants concededly offered and provided and, absent a court [*48] 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. n135 "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," n136 so DeCSS clearly is a means of circumventing a technological access control measure. n137 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.

[*50]

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." n138 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 [*51] 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. n139

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 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 [*52] 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." n140

Further, the House Commerce Committee made clear that measures based on encryption or scrambling "effectively control" access to copyrighted works, n141 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 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. n142

(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. n143 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

Perhaps the centerpiece of defendants' statutory position is the contention that DeCSS was not created for the purpose of pirating copyrighted motion pictures. [*55] 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. n144 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" n145 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 [*56] to copyrighted works. n146 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 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 [*57] 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. . . .

d. *Fair use*

[D]efendants rely on the doctrine of fair use. Stated in its most general terms, the doctrine, now codified in Section 107 of the Copyright Act, n158 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 [*65] of the work. n159 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. n160 This latter point means that certain uses 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." n161 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, [*67] 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 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. n162 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. ..." n163 By doing so, it left "the traditional defenses to copyright infringement, including fair use, ... fully applicable" provided "the access is authorized." n164

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 [*69] adversely by Section 1201(a)(1). n165

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.
n166

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.* [*70] n167 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. n168 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 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." n169 Indeed, Congress explicitly noted that Section 1201 does not incorporate

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.

* * *

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 [*148] 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