Leon P. Gold (LG-1434)
William M. Hart (WH-1604)
PROSKAUER ROSE LLP
1585 Broadway
New York, New York 10036
(212) 969-3000 Telephone
(212) 969-2900 Facsimile

Jon A. Baumgarten (pro hac vice admission to be applied for)
PROSKAUER ROSE LLP
1233 20th Street, N.W., Suite 800
Washington, DC 20036-2396
(202) 416-6800 Telephone
(202) 416-6899 Facsimile

Attorneys for Plaintiffs

UNITED STATES DISTRICT COURT

SOUTHERN DISTRICT OF NEW YORK

UNIVERSAL CITY STUDIOS, INC.; PARAMOUNT PICTURES CORPORATION; METRO-GOLDWYN-MAYER STUDIOS INC.; TRISTAR PICTURES, INC.; COLUMBIA PICTURES INDUSTRIES, INC.; TIME WARNER ENTERTAINMENT CO., L.P.; DISNEY ENTERPRISES, INC.; AND TWENTIETH CENTURY FOX FILM CORPORATION, Plaintiffs, v. SHAWN C. REIMERDES, ERIC CORLEY A/K/A "EMMANUEL GOLDSTEIN" AND ROMAN KAZAN, Defendants.	00 Civ. _____ **MEMORANDUM OF LAW IN SUPPORT OF PLAINTIFFS' APPLICATION FOR A PRELIMINARY INJUNCTION**

PRELIMINARY STATEMENT

Defendants are illegally distributing through their respective Internet web sites, a software utility which allows Plaintiffs' encrypted, copyrighted movies contained on digital versatile discs ("DVDs.") to be "decrypted," and freely copied. This utility, called "DeCSS," circumvents the proprietary Contents Scrambling System ("CSS") that protects all of the Plaintiffs' films released in the DVD format. Defendants' distribution of this utility plainly violates the "anti-circumvention" provisions of the Digital Millennium Copyright Act ("DMCA"), which were enacted, inter alia, to protect the technological measures copyright owners put in place to prevent unauthorized access to, and infringement of, their works.

Defendants are participating in a concerted effort to proliferate DeCSS via the Internet, and have made, in some cases, brazen invitations to others to engage in motion picture piracy. (See Declaration of Bruce E. Boyden, Esq., dated January 13, 2000, Exs. 1, 20 ("Boyden Decl.")) The sole function of DeCSS is to decrypt and unscramble DVD contents. As a result, Plaintiffs' movies may be perfectly copied innumerable times and then posted to, or transferred via, the Internet, thereby harming any potential market for them.

Defendants' acts are part of a larger effort by certain computer "hacker" groups with open disdain for the motion picture studios, copyright, and the law to broadly distribute DeCSS so that, according to their misguided beliefs, no courts or law enforcement agencies will be able to stop their illegal conduct. For example, one "netizen" has sponsored a widely-publicized "great international source code distribution contest," offering prizes to the Internet participants who distribute the greatest number of copies of software like DeCSS. (See Boyden Decl. Ex. 10.) Defendants virtually invite suit in the mistaken beliefs that: (1) their conduct is an exercise of free speech; and (2) by proliferating DeCSS in an explosive manner, their numbers will discourage

Plaintiffs, and this Court, from enforcing important federal law provisions enacted precisely to prevent such activities.[1]

Consistent with the United States' obligations under the recently ratified World Intellectual Property Organization ("WIPO") treaties on copyright, the DMCA was designed to bring United States copyright laws into the digital age. The DMCA provisions prohibiting circumvention of encryption systems such as CSS were prompted by the need to protect copyrighted content stored on digital media from unlawful access.[2] Congress clearly recognized that "[d]ue to the ease with which digital works can be copied and distributed worldwide virtually

---

[1] (See Boyden Decl. Ex. 10.) Defendant Corley tells visitors to his site that "you can help" by copying the DeCSS file and "mirroring" it; i.e., by making it available on their own sites for download. (Id. Ex. 7 (www.2600.com/news/1999/1227-help.html at 1).) Defendant Reimerdes defies the authorities to shut down his site promoting the free copying of DVDs, stating that "there is no lawyer that can prevent us," and announces: "Notice: The DVD Copy Control Association are cocksuckers!" (Id. Ex. 1.) A third "netizen" encourages visitors to download the DeCSS "contraband," and claims "you can't stop us all." (Id. Ex. 25.) One hacker from Arizona proclaims "dont [sic] fucking complain, you fucking deserve it, you rich fucking snobs." (Id. Ex. 23.) Another declares: "We are hackers, hear us roar." (Id. Ex. 21 at 1.)

[2] See 1 MELVILLE B. NIMMER & DAVID NIMMER, NIMMER ON COPYRIGHT at §12A.03[c] at 12-27 n.105 (1999) (hereinafter "NIMMER") (citing "encryption on a DVD" as an example of an "access control").

instantaneously," copyright owners, understandably, would hesitate to make their works readily available on digital media without strong protections. See S. Rep. No. 105-190 at 8 (1998). Thus, "[the DMCA] encourages technological solutions, in general, by enforcing private parties' use of technological protection measures with legal sanctions for circumvention and for producing and distributing products . . . that are aimed at circumventing" protection measures like CSS. Id. at 11. The fact that DeCSS is an unlawful "circumvention device" within the meaning of the DMCA is beyond dispute.

Absent effective enforcement of the DMCA anti-circumvention provisions, the harm to Plaintiffs is obvious and will be incalculable. Plaintiffs' most valuable assets are now being exposed to digital proliferation without their authorization or control. If this Court fails to issue a preliminary injunction, it will be removing the most formidable obstacle Congress put into place to protect against digital piracy. Because the equities are overwhelmingly in Plaintiff's favor, an immediate injunction is warranted.

STATEMENT OF RELEVANT FACTS[3]

A. THE PLAINTIFF COPYRIGHT HOLDERS AND THE ADVENT OF DVD TECHNOLOGY

Plaintiffs in this action are the world's leading producers and distributors of numerous commercially successful and award-winning motion pictures. (Complaint ¶ 10.) Plaintiffs' respective reputations as producers and distributors of motion pictures are widely and favorably known in this judicial district, throughout the United States, and around the world.

Plaintiffs distribute films theatrically, via television broadcast, and on portable media such as videocassette tapes and digital versatile discs ("DVDs"). (Id. ¶ 10.) DVDs are 5-inch wide discs with the storage capacity to hold a full-length motion picture, and they represent the most current technological advancement for private home viewing of motion pictures. (Id. ¶ 17.) DVDs can be played either on dedicated, free standing devices (i.e., "DVD players") or on personal computers ("PCs") configured with a DVD ROM "drive" and additional hardware or software modules, sometimes referred to as "media players." (Id. ¶ 18.) The audiovisual information on DVDs is stored digitally, which provides a significant improvement in the clarity and the overall quality of the motion picture when played on a television screen or computer monitor. (Id. ¶ 19.) In contrast to an analog-format VHS tape, motion pictures embodied on DVDs can be copied with no significant degradation of picture and sound clarity or overall quality. (Id.) Thus, without some form of protection through encryption, unauthorized copies of

---

[3] The facts relevant to this motion are set forth in the accompanying declarations of Fritz Attaway, dated January 13, 2000 (the "Attaway Decl."), Michael Ostroff, dated January 13, 2000 (the "Ostroff Decl."), and the Boyden Decl.

motion pictures from DVDs can be easily made, stored on computer tape or disk drives, and/or repeatedly duplicated for unlawful sale, transfer, or exchange, including over the Internet.

Plaintiffs own or control the United States copyrights in various motion pictures embodied on DVDs, including such recent blockbusters as "Titanic" and "The Matrix." (Id. ¶ 10.) Plaintiffs are the leading producers and distributors of motion pictures in the DVD format, and approximately 4,000 titles have been released in the United States on DVD to date. (Id.) Current estimates place DVD sales at over 1,000,000 units per week. (Id.)

B. DVD SECURITY AND ANTI-PIRACY TECHNOLOGY

Because of the potential to create unauthorized, high-quality copies of motion pictures from DVDs, the leading motion picture companies, including Plaintiffs herein, insisted on the development of a copy protection and access control system before allowing their copyrighted motion pictures to be reproduced on the new medium. (Complaint ¶ 20; Attaway Decl. ¶ 4.) To address this concern, Matsushita Electronics Industrial Co., Ltd. ("MEI") and Toshiba Corporation developed a proprietary system called the Contents Scrambling System ("CSS"), which became the widely accepted standard for protecting copyrighted motion pictures, and other copyrightable content, embodied on DVDs. (Complaint ¶ 20.) CSS includes elements of encryption and other computer security and authentication technology, which require DVD players and PC-based DVD drives to incorporate software "keys" in order to descramble and intelligibly play movies from DVDs. (Complaint ¶ 20; Attaway Decl. ¶ 5.) Thus, CSS both encrypts and scrambles the digital signals embodying the copyrighted motion picture — which, effectively, disallows even playback of the DVD without an encryption "key" — and prevents copying of the contents of DVDs. (Complaint ¶ 20.)

C. THE "CRACKING" OF CSS AND DISSEMINATION OF "DeCSS"

On or about October 25, 1999, the source code for a software utility aptly titled "DeCSS" (presumably, the first syllable refers to the program's ability to "de-scramble" or "de-crypt" the CSS program) appeared on an Internet web site operated by a Norwegian, Jon Johansen.[4] (Complaint ¶ 22; Attaway Decl. ¶ 7.) DeCSS allows an individual to decode the CSS encryption on a DVD movie, and also allows the user to copy a "decrypted" file embodying the movie on his or her hard drive. (Complaint ¶ 22; Attaway Decl. ¶ 7.)

Immediately after the DeCSS hack appeared on the Internet in the United States, the Motion Picture Association of America ("MPAA"), on behalf of its copyright holder members, began to take action under the provisions of the DMCA. (Attaway Decl. ¶ 8.) Such action included sending demands to various Internet service providers to remove DeCSS from their Internet systems and, at least where their identities were known, demands to individuals to remove their DeCSS postings and refrain from such conduct. (Id.) These efforts succeeded in causing the removal of quite a number of Internet postings of DeCSS. (Id.) However, the proliferation of these postings recently has increased dramatically, due to a concerted effort by various individuals, including the Defendants, within the United States.

D. THE DVD CCA TRADE SECRET ACTION AND THE DEFENDANTS' ILLEGAL ACTIVITIES

[4] Johansen is believed to be a member of a computer "hacker" group called "Masters of Reverse Engineering " or "MoRE." (See Boyden Decl. Ex. 7 (www.2600.com/news/1999/1112.html at 1).) The exploits of Johansen and MoRE are touted on Internet websites such as "www.2600.com" that are popular among the hacker community. (Id.)

The licensor of the CSS system, the CCA,[5] recently commenced in California state court an action, on trade secret grounds, to prevent the unlawful use and disclosure of any of its confidential information embodied in DeCSS. (Attaway Decl. ¶ 9.) Plaintiffs are not parties to that case and, indeed, have no standing to assert any such trade secret claim. The California Superior Court denied the CCA's application for a TRO on December 29, 1999. (Id.) Immediately thereafter, the proliferation and dissemination of the DeCSS utility facility exploded.

In an apparent effort to influence the outcome of any future court proceedings, various Internet sites have encouraged parties to "help" by making copies or "mirrors" of sites containing DeCSS. (See Boyden Decl. Exs. 10, 11, 13, 23.) The Defendants are now offering DeCSS via the Internet accompanied by statements like:[6]

- "Yes, you can trade DVD movie files over the Internet . . . You can break the encryption on any DVD and allow users to copy the contents of a DVD onto the a [sic] hard drive or alternative media! Notice: The DVD Copy Control Association are cocksuckers!";
- "**How To Find/Trade FREE DVD Movies Online** . . . people gather online in impromptu communities and trade these digital copies through one-to-one file transfers and group chatting" (emphasis in original); and

---

5 The "CCA" is the DVD Copy Control Association, which holds the proprietary rights to the CSS encryption system. (Attaway Decl. ¶ 9.)

6 (See Boyden Decl. Exs. 1, 7 (www.2600.com/news/1999/1227-help.html, at 1).)

- "[I]t's especially important that as many of you as possible all throughout the world take and mirror [the DeCSS] files . . . ."

DeCSS is plainly an unlawful circumvention device within the meaning of the DMCA, and is immediately enjoinable as such. It is irrelevant whether or not any of the Defendants personally was engaged in any purloining of CSS trade secrets, or in the unauthorized decryption or duplication of any of Plaintiffs' DVD movies. Defendants are providing the "burglary keys" in violation of the anti-circumvention provisions of the federal copyright law, and their claimed belief that they are permitted to do so (as an exercise of free speech or otherwise) is no defense.

ARGUMENT

Plaintiffs more than satisfy the standard for a preliminary injunction, which requires the moving party to demonstrate: (1) the threat of irreparable injury if the injunction is not granted; and (2) either (a) a likelihood of success on the merits of its claims or (b) sufficiently serious questions going to the merits to make them a fair ground for litigation and that the balance of equities tips decidedly in the movant's favor. Genesee Brewing Co. v. Stroh Brewing Co., 124 F.3d 137, 142 (2d Cir. 1997); Tom Doherty Assocs. v. Saban Entertainment, Inc., 60 F.3d 27, 33 (2d Cir. 1995).

PLAINTIFFS ARE ENTITLED TO A PRELIMINARY INJUNCTION

A. PLAINTIFFS ARE LIKELY TO SUCCEED ON THE MERITS OF THEIR DMCA CLAIM BECAUSE DEFENDANTS' ACTIVITIES CLEARLY VIOLATE THE ANTI-CIRCUMVENTION PROVISIONS OF THE COPYRIGHT ACT

One of the primary objectives of the DMCA was to bring United States copyright law in line with the World Intellectual Property Organization ("WIPO") treaties on copyright, which were ratified by the United States. See S. Rep. No. 105-190, at 8 (1998). The WIPO treaties imposed an obligation on member countries to "provide 'legal protection and effective legal remedies' against circumventing technological measures, e.g., encryption and password protection, that are used by copyright owners to protect their works from piracy . . . ." Id. at 10-11.

Such protection was essential to bring United States copyright law into the digital age, and to provide a legal framework for copyrighted creative works to be offered to the public in digital formats without the substantial risk of wholesale, high-tech infringement. See NIMMER § 12A-03[B][1] at 12A-12. Key provisions of the DMCA (as codified in the Copyright Act at 17 U.S.C. § 1201, et seq.) unambiguously prohibit the circumvention of copyright protection systems like CSS. These provisions were designed, inter alia, to protect the "encryption on a DVD which acts as 'access control.'" See NIMMER § 12A.03[C] at 12A-27 n.105.

Specifically, Title 17 U.S.C. § 1201(a)(2) provides that:

> [n]o person shall manufacture, import, offer to the public, provide, or otherwise traffic in any technology, product, service, device, component, or part thereof, that —
>
> (A) is primarily designed or produced for the purpose of circumventing a technological measure that effectively controls access to a work protected under this title;
>
> (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 this title; 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 this title.

17 U.S.C. § 1201(a)(2) (1999). Only one of these conditions need be satisfied in order for this Court to find a violation. See S. Rep. No. 105-190, at 29 ("For a technology, product, service, device, component, or part thereof to be prohibited under this subsection, *one* of three conditions must be met.") (emphasis supplied). The anti-circumvention provisions directed toward "access controls" are designed to prevent the electronic "equivalent [of] breaking into a castle." See NIMMER § 12A.03[D][1], at 12A.-29; H.R. Rep. No. 105-551, pt. 1, at 17 (1998) ("The act of circumventing a technological protection measure put in place by a copyright owner to control access to a copyrighted work is the electronic equivalent of breaking into a locked room in order to obtain a copy of a book").[7]

Under the statute, to "circumvent a technological measure" means to "descramble a scrambled work, to decrypt an encrypted work, or otherwise to avoid, bypass, remove, deactivate, or impair a technological measure, without the authority of the copyright owner." 17 U.S.C. § 1201(a)(3)(A) (1999). Further, "a technological measure 'effectively controls access to a work' [within the meaning of section 1201(a)(2)] 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 the work." See 17 U.S.C. § 1201(a)(3)(B) (1999).

1. CSS Is a "Technological Measure That Effectively Controls Access to" Plaintiffs' Copyrighted Works

There is no question that CSS is a technological measure that was designed and employed to control access to Plaintiffs' copyrighted works and, thus, is entitled to protection under the

[7] See also Jane C. Ginsburg, Copyright Legislation For The "Digital Millennium," 23 Colum.-VLA J.L. & Arts 137, 140-42 (1999) (hereinafter "Ginsburg") (using an example of a user password and hardware verification device as methods of controlling "access" to a copyrighted work through technological measures).

anti-circumvention statute. Because the CSS encryption methodology requires a software "key" in order to effect playback of the copyrighted motion picture on a DVD, CSS qualifies as an "access" control measure within the meaning of 17 U.S.C. § 1201(a)(2).[8]

Congress expressly declined to mandate any technical standard for the "effectiveness" of the "technological measure" for it to be entitled to protection under Section 1201(a):

> Any effort to read into this bill what is not there -- a statutory definition of "technological measure" -- *or to define in terms of particular technologies what constitutes an "effective" measure,* could inadvertently deprive legal protection to some of the copy or access control technologies that are or will be in widespread use for the protection of both digital and analog formats.

See STAFF OF HOUSE OF REPRESENTATIVES COMM. ON THE JUDICIARY, 105TH CONG., 2D SESS., SECTION-BY-SECTION ANALYSIS OF H.R. 2281 AS PASSED BY THE UNITED STATES HOUSE OF REPRESENTATIVES ON AUGUST 4, 1998, at 9 (Comm. Print 1998) [hereinafter "HOUSE JUD. COMM. REP."] (emphasis supplied).

---

[8] Ginsburg at 140-41 (discussing the concept of "access" controls protected under 17 U.S.C. § 1201(a)(2) and explaining that, to avoid running afoul of the statute, "the user may not . . . circumvent a technological measure that controls the user's ability to apprehend the work"); see also NIMMER 12A.03[C], at 12A-27 n.105.

Indeed, "[a] password fits [the] paradigm" of an "effective technological measure." See NIMMER § 12A.03[A][1][b], at 12A-17 (citing S. Rep. No. 105-190, at 12-13). Thus, any argument that, because a group of hackers was able to "break" the CSS encryption, CSS is undeserving of protection under the anti-circumvention provisions of the DMCA, defies common sense and the plain meaning of the statute.[9]

2. "DeCSS" Unlawfully Circumvents CSS

The Senate Report accompanying the DMCA explains that, "if unauthorized access to a copyrighted work is effectively prevented through use of a password, *it would be a violation of this section to defeat or bypass the password and to make the means to do so*, as long as the primary purpose of the means was to perform this kind of act." See S. Rep. No. 105-190, at 11 (emphasis supplied).

---

[9] "Throughout the legislative process, the phrase 'technological measure' . . . has been treated in [the House version of the DMCA] in terms of the *function such a measure would perform, rather than the specific technology to be used or the means for developing it* . . . The practical, common-sense approach taken by [the DMCA] is that if, in the ordinary course of its operation, a technology actually works in the defined ways to control access to a work, or to control copying, distribution, public performance, or the exercise of other exclusive rights in 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." HOUSE JUD. COMM. REP., at 10. (emphasis supplied).

That is precisely what Defendants have done here. They are providing to the public (and, unless enjoined by this Court, will continue to provide) the "password" or "keys" to "unlock" DVD encryption in violation of Section 1201(a)(2).

3. Defendants' Acts of Offering to the Public, Providing, or Otherwise Trafficking in DeCSS Are in Direct Violation of the Statute.

Defendants' acts of providing DeCSS to the public blatantly violate the statutory mandate that no person shall, inter alia, "offer to the public, provide, or otherwise traffic in any technology, product, service, device, component, or part thereof" that circumvents an access control device such as CSS. "While this legislation is aimed primarily at 'black boxes' that have virtually no legitimate uses, trafficking in *any product or service* that meets one or more of the three points in [the 17 U.S.C.§ 1201(a)(2)] test could lead to liability. It is not required to prove that the device in question was 'expressly intended to facilitate circumvention.'" HOUSE JUD. COMM. REP., at 9 (emphasis supplied). See also Ginsburg at 144 ("If users may not directly defeat access controls, it follows that third parties should not enable users to gain unauthorized access to copyrighted works by providing devices or services (etc.) that are designed to circumvent access controls. Indeed *the principal targets of the DMCA are the providers of circumvention devices, services, etc*.") (emphasis supplied).

There is no question that Defendants are providing a circumvention device to the public within the plain meaning of the statute. (See Boyden Decl. Ex. 1 ("[With DeCSS] [y]ou can break the encryption on any DVD and allow users to copy the contents of a DVD onto the a [sic] hard drive or alternative media!"); id. at Ex. 7 ("it's especially important that as many of you as possible all throughout the world take and mirror [the DeCSS] files"); see also id. at Ex. 21 ("The only solution was to really break the encryption method").)

4. DeCSS Has the Primary Purpose of Circumventing CSS

and Has at Most Only a Limited Commercially Significant Purpose or Use Other than to Circumvent.

DeCSS unquestionably was designed and disseminated with the "primary purpose" of circumventing the CSS encryption methodology within the meaning of 17 U.S.C. §1201(a)(2)(A). In basic terms, as widely reported on Internet web pages and other on-line reports accompanying the initial posting of the utility, DeCSS copies a DVD file encrypted with the CSS algorithm and allows the user to save the file back to a hard drive, *minus the encryption*. (See Boyden Decl. Exs. 1, 15-16, 17 (page titled "What Exactly is DeCSS?").)

Moreover, the condition that a device must have "only [a] limited commercially significant purpose or use other than to circumvent," see 17 U.S.C. § 1202(a)(2)(B), "imposes an objective criterion: whatever the device's producer intended, how is the device in fact being used?" See Ginsburg at 145. As discussed above, that question is easily answered given Defendants' provision of the DeCSS utility, and the other veritable "instruction manuals" available on-line for how to "crack open," decrypt, and copy Plaintiffs' DVDs.[10]

[10] For example, a bulletin board on the web site "www.pzcommunications.com" noted that "[o]ne of our visitors has informed us of a solution to the size of the [decrypted DVD] file problem for storage. OnStream's line of high performance, drive letter access tape drives allow you to store anywhere from 4 to 6 full quality, bit for bit *unprotected* copies of DVD's [sic] on one OnStream tape. No more flipping disk [sic], no more shuffling

through menus, no more region codes, just hit play on your Software DVD player and away it goes!" (See Boyden Decl. Ex. 17 (page titled "What About the Size of the Decrypted Movie Files," at 1) (emphasis supplied).) Another www.pzcommunications.com visitor noted that "I can rip up to 5 full length DVDs and play them back directly from the [OnStream] tape drive. Ripping time for an average DVD [is] about 30 minutes when ripping directly to the OnStream drive letter (seems to be limited by the speed of the DVD-ROM I have." (Id.)

Plaintiffs do not have to show copyright infringement as an element of their anti-circumvention claim, although the potential for such additional claims is clear. To be sure, the fact that Defendants are offering or providing DeCSS — a prohibited circumvention device — to the public constitutes a violation of Section 1201(a)(2) and must be enjoined. Any arguments Defendants may pose concerning other theoretically "legitimate" applications of DeCSS are irrelevant, and do not constitute a defense to their violation of 17 U.S.C. § 1201(a)(2).[11]

---

[11] For example, some Internet discussions have, as a pretext, the possible "research utility" of the DeCSS hack. However, none of the Defendants claims to have created DeCSS; they are merely proliferating it. As such, they cannot benefit from the extremely narrow "reverse engineering" or "encryption research" exemptions that are set forth in 17 U.S.C. § 1201(f) and (g). See S. Rep. No. 105-190, at 33 ("Recognizing . . . that making such circumvention information or tools generally available [in the name of reverse engineering] would undermine the objectives of the [DMCA], this section imposes strict limitations"); see also Ginsburg at 149 ("[R]everse engineering should not become a pretext for defeating access controls in order to acquire computer programs for free, or in order to make infringing copies of the program."). Even more fundamentally, "[the reverse engineering exemption] applies to computer programs as such, regardless of their medium

5. Defendants' Activities Are Not Protected under the First Amendment.

Any defense based upon Defendants' alleged "entitlement" under the First Amendment to traffic in decryption devices should be given short shrift by this Court. The DMCA is, itself, based upon constitutional imperatives, and Congress took into account any First Amendment considerations when it enacted the DMCA. See 17 U.S.C. §§ 1201(c)(4) and 1203(b)(1). "[T]he first amendment is not a license to trammel on legally recognized rights in intellectual property'. . . Since the Copyright Act is the congressional implementation of a constitutional directive . . . , copyright interests also must be guarded under the Constitution." Cable/Home Communication Corp. v. Network Prod., 902 F.2d 829, 849 (11th Cir. 1990) (citation omitted); see also United Video, Inc. v. F.C.C., 890 F.2d 1173, 1190-91 (D.C. Cir. 1989) ("The Constitution grants Congress the power to secure for limited times to authors the exclusive right

---

of fixation and not to works generally such as music or audiovisual works, which may be fixed and distributed in digital form." S. Rep. No. 105-190, at 33. Further, "out of apparent concern that 'encryption research' could degenerate into a pretext for indiscriminate hacking of access controls, [§ 1201(g)] further attempts to restrict the class of persons qualified for the exemption by listing factors [for courts] to consider: whether the information derived from the research was disseminated in a manner 'reasonably calculated to advance the state of knowledge or development or encryption technology' or whether instead it 'facilitates infringement' [or, among others,] whether and when the results of the research are disclosed to the copyright owner." Ginsburg at 150 (discussing 17 U.S.C. § 1201(g)).

to their works, and this power generally supersedes the first amendment rights of those who wish to use another's copyrighted work").

The First Amendment does not prohibit Congress from preventing Defendants' proliferation of DeCSS. Just as the federal and state governments may protect private property by criminalizing breaking and entering, or the sale of specialized tools for picking locks,[12] Congress also can protect intellectual property stored on digital media by criminalizing the distribution of devices that provide the keys to the proverbial "DVD castle."

B. PLAINTIFFS ARE BEING, AND WILL CONTINUE TO BE, IRREPARABLY HARMED BY DEFENDANTS' DISSEMINATION OF CIRCUMVENTION DEVICES SUCH AS "DeCSS"

[12] See generally 18 U.S.C. § 642 (prohibiting theft or embezzling tools and devices used for counterfeiting purposes); see also N.Y. Pen. Law § 140.35 (criminalizing possession of burglary tools); Conn. Gen. Stat. Ann. § 53a-106 (1999) (same); Or. Rev. Stat. § 164.235 (1998) (same).

The harm to Plaintiffs from Defendants' provision of DeCSS to the public, if left unchecked by this Court, will be enormous. Given the substantial investments already made in the DVD format and the CSS encryption standard, Plaintiffs are faced with a Hobson's Choice: they can continue releasing existing and new films on DVDs with the potential, if not the certainty, that each one may be freely decrypted and copied, thereby exposing Plaintiffs' most valuable assets to widespread, unrestricted commercial copying;[13] or, Plaintiffs are faced with the prospect of limiting their movie releases on DVDs. (Attaway Decl. ¶¶ 12-14.) Obviously, neither choice is attractive because the release of films on DVDs represents an important source of revenue to offset the considerable expenses of film production, distribution, and marketing. (Attaway Decl. ¶¶ 14.) If the proliferation of DeCSS is left unchecked, it will greatly diminish the economic value of Plaintiffs' motion pictures, thereby reducing the amount of investment that can be made in those pictures. (Id.) The result will be widespread economic harm not only to the motion picture studios, but also to those who work in the motion picture industry. (Id.)

Moreover, the harm to consumers, who also have made substantial investments in DVD software and hardware, is equally significant. The losses from unauthorized copying of Plaintiffs' films in analog formats are immense, with industry estimates putting the figure in the billions of dollars annually. (Id. ¶ 13.) Digital copying and proliferation presents an even more formidable threat. (Id.)

---

[13] Moreover, the emergence of mainstream DeCSS products outside of the hacker community will only ensure that such unauthorized access and copying is not confined to the fringe elements of the Internet.

Ultimately, the consuming public also will suffer should the Court fail to enforce the federal anti-circumvention provisions, since the latest digital, "high definition" technologies for the delivery of entertainment content may not be released so quickly. For example, the introduction of musical works on DVDs, already has been postponed because of the proliferation of DeCSS. (See Ostroff Decl. ¶¶ 2-3.)

Given the potential for exponential proliferation of unauthorized copying through advances in digital technology, Congress deemed it essential — indeed, mandatory in light of the WIPO treaties — to put legal protections in place for the tools that copyright owners utilize to prevent unauthorized access to their copyrighted works in digital formats. Once a violation of the anti-circumvention provisions has been established, Plaintiffs are entitled to injunctive relief to prevent the proliferation of unlawful circumvention devices from spreading. See 17 U.S.C. § 1203(b)(1).[14] This is because, as a practical matter, stopping the electronic reproduction and transmission of unauthorized copies of copyrighted works in the digital environment is extremely difficult, and has been recognized as such both by Congress and the courts. See, e.g., Sega Enters., Ltd. v. Maphia, 857 F. Supp. 679, 688 (N.D. Cal. 1994) (noting that the existence of 45,000 Internet bulletin boards, like the defendant's, which posted pirated video games, made it "obvious" that unauthorized copying of plaintiff's video game software would have a "substantial and immeasurable adverse effect on the market for [plaintiff's] copyrighted works"); S. Rep. No. 105-190, at 3 (recognizing that the "ease with which digital works can be distributed worldwide virtually instantaneously" will cause copyright owners to hesitate before making their works

[14] Under well-established copyright jurisprudence, once a plaintiff establishes a prima facie case on the merits of a Copyright Act claim, courts generally presume irreparable harm flowing therefrom. See Sun Microsystems, Inc. v. Microsoft Corp., 188 F.3d 1115 (9th Cir. 1999); Fisher-Price, Inc. v. Well-Made Toy Mfg. Corp., 25 F.3d 119 (2d Cir. 1994).

available in digital form). Any purported harm suffered by Defendants as a result of such an injunction is, by comparison, non-existent.[15]

C. ALTERNATIVELY, PLAINTIFFS' APPLICATION PRESENTS SUFFICIENTLY SERIOUS QUESTIONS GOING TO THE MERITS OF THEIR CLAIMS, AND THE BALANCE OF EQUITIES FAVORS PLAINTIFFS.

Plaintiffs' entitlement to injunctive relief is also established by showing sufficiently serious questions going to the merits to make them a fair ground for litigation, and a balance of equities tipping decidedly in their favor. See Genesee Brewing Co., 124 F.3d at 142, Jim Doherty Assocs., 60 F.3d at 33. Plaintiffs have demonstrated the great hardship threatened by Defendants' conduct, including the enormous irreparable harm threatened by widespread distribution of DeCSS should an injunction be denied. Plaintiffs respectfully submit there is no harm resulting to Defendants from the imposition of an injunction prohibiting their provision of an unlawful circumvention device to the public.

This case presents a very basic but critical need for the application of recent key amendments to the Copyright Act that were necessitated by the demands of digital technological innovation. As discussed, the DMCA anti-circumvention provisions were enacted precisely to prevent the sort of conduct engaged in by Defendants. If Defendants' actions are permitted to go

---

[15] Defendants' actions not only give rise to civil liability, but to serious potential criminal liability as well. See 17 U.S.C. § 1204 (providing that violations of § 1201 "willfully and for purposes of commercial advantage or private financial gain" are subject to fine and imprisonment.) The definition of "commercial advantage or private financial gain" in the Copyright Act was amended by the "Net Act" in 1997 to impose criminal liability where no commercial gain is sought or obtained by the offender. See 17 U.S.C. § 506(a)(2).

unchecked, the hardship to Plaintiffs will be grave and the balance of equities does not merely tip, but topples, in Plaintiffs' favor. Although Plaintiffs submit that they have more than amply demonstrated a probability of success on the merits, there certainly are sufficiently serious questions going to the merits of Plaintiffs' claims to justify the entry of immediate injunctive relief.

Given the relative equities at stake, including the lack of any cognizable harm to Defendants from the imposition of an appropriate injunction, such relief is mandated.

CONCLUSION

For the foregoing reasons, Plaintiffs' application for a preliminary injunction should be granted in all respects.

Dated: New York, New York
January 14, 2000

PROSKAUER ROSE LLP

By: _____

Leon P. Gold (LG-1434)
William M. Hart (WH-1604)
1585 Broadway
New York, New York 10036
(212) 969-3000 Telephone
(212) 969-2900 Facsimile

- and -

Jon A. Baumgarten
(pro hac vice admission to be applied for)
PROSKAUER ROSE LLP
1233 20 Street, N.W., Suite 800
Washington, DC 20036-2396
(202) 416-6800 Telephone
(202) 416-6899 Facsimile

Attorneys for Plaintiffs

TABLE OF CONTENTS