Anti-circumvention rules and fair use

By Lev Ginsburg

Spring, 2002

Los Angeles, California

On October 28, 1998, President Clinton signed the Digital Millennium Copyright Act (the "**DMCA**"), which includes several provisions in its Section 1201 that restrict one's ability to lawfully circumvent a copyright holder's copyright protection technologies.[1] This paper argues that Section 1201 should not be construed so as to deny defendants the ability to raise the fair use defense.

The analysis begins by exploring and defining the rule set forth in *Reimerdes*[2], the first major action brought under those provisions of the DMCA. *Reimerdes* held, *inter alia*, that fair use defenses are not permitted in Section 1201 actions.

Part II discusses the implications of the *Reimerdes* decision and makes several suggestions as why Section 1201 should be construed to permit a defendant to raise a fair use defense to a Section 1201 action. Part II's focus is my argument that Section 1201 violations are essentially allegations of contributory copyright infringement to which the

[1] Copyright Act, 17 U.S.C. § 1201 (West, WESTLAW through July 2002 legislation).
[2] Universal City Studios, Inc. v. Reimerdes, 111 F. Supp. 2d 294 (2000).

fair use doctrine should apply. Moreover, Section 1201's very language permits fair uses of copyrighted material that is encrypted with anti-circumvention technology.

Finally, Part III proposes several hypothetical situations that illustrate some of the tensions caused by *Reimerdes*'s interpretation of Section 1201 and support the assertions set forth in Part II.

PART I

Factual background

To protect their intellectual properties, the film studios that distribute films on digital versatile disks ("**DVDs**") encrypt each DVD's copyrighted content using a technology they call the "content scramble system" ("**CSS**"). CSS 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 then play back, but not copy, motion pictures on DVDs."[3] CSS technology has been licensed to hundreds of manufacturers around the world.[4]

In *Reimerdes*, the eight major United States motion picture studios brought an action to enjoin defendant Eric Corley,[5] a "leader of the computer hacker community,"[6]

[3] . *Id*. at 308 .
[4] *See id.*
[5] Mr. Reimerdes and the other defendant, Roman Kazan, settled with the studios following the grant of the preliminary injunction by entering into consent decrees. *See id*. at 312 n.91.

from posting code[7] for a computer program called "DeCSS"[8] on his website.[9] DeCSS "enables users to break the CSS copy protection system and hence to view DVDs on unlicensed players and make digital copies of DVD movies."[10] Above and beyond their concerns about the unauthorized appropriation of their intellectual properties, the studios are particularly concerned by the fact that with respect to digital media such as DVDs, all copies, whether or not authorized, are of a quality identical to that of the "original" material from which the copy was made.[11]

The lower court granted plaintiffs' motion for a preliminary injunction barring Corley from posting DeCSS on his website. Following the issuance of this injunction, Corley removed DeCSS from his website, but continued to provide "links" to other websites that offered DeCSS.[12]

---

[6] *Id*. at 308.

[7] Corley posted both "object" and "source" code for DeCSS. Source code is the text of computer programming language(s) that use symbols and syntax to convey meaning. Source code is translated into object code, which is a string of numbers that a computer can "read" and perform in response to. Some source code is quite similar to spoken language, while some more closely resembles the strings of numbers of object code. *See id*. at 306 for a more detailed explanation of the relationship between these two varieties of computer code.

[8] DeCSS was created in September, 1999, by a fifteen year-old Norwegian named Jon Johansen, who, along with some associates, "reverse engineered a licensed DVD player and discovered the CSS encryption algorithm and keys." *Id*. at 311.

[9] In the months following DeCSS's initial appearance on Johansen's own website, DeCSS became widely available on the Internet. *See id*. As of this writing, hundreds, if not thousands of websites purport to offer DeCSS for download, along with similar programs derived from DeCSS-like techniques. *See id*. at n.82.

[10] *Id*. at 308.

[11] This is particularly so in light of the fact that DVDs decrypted with DeCSS can be digitally compressed to a size that allows them to be copied directly onto a common compact disc, without significant diminution in quality, for around one dollar apiece. *See id*. at 31. Accordingly, there is an added incentive for consumers to unlawfully reproduce digital DVDs as compared with analog VHS cassettes because of the higher quality of the resulting copy. The studios are therefore quite invested in protecting each DVD's digital content.

[12] *See id*. at 312. The studios amended their complaint and also sought to enjoin Corley from "linking" his post-injunction website to other websites whose webmasters quickly copied and posted DeCSS for themselves. The linking debate is an off-shoot of several First Amendment issues raised in *Reimerdes* and

Judge Kaplan's opinion summed up the facts by writing that

> [t]he net of all this is reasonably plain. DeCSS is a free, effective, and fast means of decrypting plaintiffs' DVDs and copying them to computer hard drives . . . . [T]he availability of DeCSS on the Internet effectively has compromised plaintiffs' system of copyright protection for DVDs . . . . It is analogous to the publication of a bank vault combination in a national newspaper. Even if no one uses the combination to open the vault, its mere publication has the effect of defeating the bank's security system, forcing the bank to reprogram the lock.[13]

Statutory background

In 1997, the World Intellectual Property Organization ("**WIPO**"), adopted the WIPO Copyright Treaty (the "**Treaty**"), Article 11 of which provides, in relevant part, that contracting states "shall provide adequate legal protection and effective legal remedies against [1] the circumvention of effective technological measures that are used by authors in connection with the exercise of their rights . . . and [2] restrict acts, in respect of their works, which are not authorized by the authors concerned or permitted by law."[14] From the beginning, the Treaty established what the DMCA would later institutionalize as a two-tiered approach to these issues simultaneously addressing both

---

is beyond the scope of this paper. For the court's take on Corley's linking (holding that "[d]efendants' posting and their linking amounts to very much the same thing."), see *id*. at 339.

[13] *Id*. at 315.

actual circumvention and to other unauthorized acts in connection with such circumvention.

Though the Treaty did not require Congress to pass any law in particular,[15] Congress soon began to consider these issues against the backdrop of the Treaty. A divide arose "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."[16] Congress enacted the DMCA in October, 1998, as the culmination of its process of considering the various implications of both perspectives.[17]

As Judge Kaplan's *Reimerdes* opinion pointed out, the DMCA contains two principal anti-circumvention provisions. The first, Section 1201(a)(1)(A), states that "No person shall circumvent a technological measure[18] that effectively controls access to a work[19] protected under this title,"[20] an act described by Congress as "the electronic equivalent of breaking into a locked room in order to obtain a copy of a book."[21]

---

[14] WIPO Copyright Treaty, Apr. 12, 1997, art. 11, S. Treaty Doc. No. 105-17), available at 1997 WL 447232.

[15] Congress could probably, for example, have simply passed a resolution finding that current copyright laws adequately respond to the concerns expressed in the Treaty.

[16] Universal City Studios, Inc. v. Reimerdes, 111 F. Supp. 2d 294, 316 (2000).

[17] *Id*..

[18] As used in Section 1201, "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 . . . . " Copyright Act, 17 U.S.C. § 1201(a)(3)(A).

[19] As used in Section 1201, "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 of a treatment, with the authority of the copyright owner, to gain access to the work." *See id.* § 17 U.S.C. § 1201(a)(3)(B).

[20] *Id.* § 1201(a)(1)(A).

The focus of *Reimerdes*, however, was Section 1201(a)(2),[22] which supplements Section 1201(a)(1)'s prohibition against actual circumvention by providing that

> No 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 [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].[23]

---

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

[22] Section 1201(a)(2) was the focus in *Reimerdes* because Plaintiffs had not accused Corley of using DeCSS himself to bypass plaintiffs' access control measures.

[23] Copyright Act, 17 U.S.C. § 1201(a)(2). In other words, Section 1201(a)(1) "focuses directly on wrongful conduct, rather than on those who facilitate wrongful conduct," while Section 1201(a)(2), the anti-trafficking provision, "separately bans offering or providing technology that may be used to circumvent technological means of controlling access to copyrighted works. 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." *Reimerdes*, 111 F. Supp. 2d at 319 (citations omitted).

Section 1201(c), however, has generated much confusion with respect to the applicability of fair use to Section 1201. In its entirety, Section 1201(c)(1) provides that "Nothing in this section shall affect rights, remedies, limitations, or defenses to copyright infringement, including fair use, under this title."[24] Further, Section 1201(c)(2) provides, in its entirety, that "Nothing in this section shall enlarge or diminish vicarious or contributory liability for copyright infringement in connection with any technology, product, service, device, component, or part thereof . . . ."[25]

Reimerdes

Judge Kaplan found that CSS "effectively controls access" to Plaintiffs copyrighted works, even though CSS was eventually deciphered, under the theory that "a technological measure 'effectively controls access' to a copyrighted work if its *function* is to control access."[26] Additionally, Judge Kaplan found that, in the words of Section 1201(a)(2)(A), DeCSS was designed primarily to circumvent CSS because Corley admitted that "DeCSS was created solely for the purpose of decrypting CSS - that is all it does."[27] Judge Kaplan then held that "the foregoing is sufficient to establish a *prima facie* violation of Section 1201(a)(2)(B),"[28] meaning that the court found that Plaintiffs had made a *prima facie* showing that DeCSS has only limited commercially significant

[24] Copyright Act, 17 U.S.C. § 1201(c)(1).
[25] *Id.* § 1201(c)(2).
[26] *Reimerdes,* 111 F. Supp. 2d at 318 (emphasis in original).
[27] *Id.* at 319.
[28] *Id.*

purpose or use other than to circumvent a technological measure that effectively controls access to a work protected by Section 1201.

Corley argued in his defense that his activities came within several exceptions contained in the DMCA and elsewhere in the Copyright Act, and that they also constitute fair use under Section 107 of the Copyright Act. Judge Kaplan briefly considered those arguments and found them all "entirely without merit."[29]

a) Reverse engineering under Section 1201(f)

Section 1201(f)'s "Reverse Engineering" exception[30] provides in substance that "one may circumvent or develop and employ technological means to circumvent, access control measures in order to achieve interoperability with another computer program provided that doing so does not infringe another's copyright . . . ."[31] Additionally, Section 1201(f) provides that one may make information acquired through such efforts "available to others, if the person [in question] . . . provides such information or means *solely* for the purpose of enabling interoperability of an independently created computer program with other programs, and to the extent that doing so does not constitute infringement . . . ."[32]

[29] *Id.*
[30] Copyright Act, 17 U.S.C. § 1201(f).
[31] *Reimerdes*, 111 F. Supp. 2d at 320.
[32] Copyright Act, 17 U.S.C. § 1201(f)(3) (emphasis added).

Corley contended that DeCSS was necessary to achieve interoperability between computers running the Linux operating system and DVDs and that this exception therefore is satisfied. Judge Kaplan disagreed, and held that Section 1201(f)(3) permits information acquired through reverse engineering to be made available to others only by the person who acquired the information. Because Corley didn't reverse engineer anything -- he simply lifted DeCSS from another site and posted it on his own -- he was not entitled to the exception's protections.[33]

Additionally, Judge Kaplan also found that Corley would be no better off even if he had authored DeCSS because the right to make the information available extends only to dissemination that's "solely for the purpose" of achieving "interoperability" as such term is defined in the DMCA. Judge Kaplan held that the exemption does not apply to Corley's public dissemination of DeCSS. Clearly, Corley did not post DeCSS "solely" to achieve interoperability with Linux or anything else.[34]

b) Encryption research under Section 1201(g)

Next, Corley argued that his conduct was protected by Section 1201(g)'s encryption research exemption.[35] Judge Kaplan pointed out that in determining whether

[33] Reimerdes, 111 F. Supp. 2d at 320.
[34] *Id.*
[35] Section 1201(g)(4) provides in relevant part that:

> Notwithstanding the provisions of subsection (a)(2), it is not a violation of that subsection for a person to--

one is engaged in good faith encryption research protected under this exemption, "the Court is instructed to consider factors including [1] whether the results of the putative encryption research are disseminated in a manner designed to advance the state of knowledge of encryption technology versus facilitation of copyright infringement, [2] whether the person in question is engaged in legitimate study of or work in encryption, and [3] whether the results of the research are communicated in a timely fashion to the copyright owner."[36]

When applying those principles to the facts before him, Judge Kaplan determined that Corley had not engaged in any good faith encryption research because (1) he simply posted DeCSS for "all the world" to see; (2) he made no effort to provide the results of

---

> (A) develop and employ technological means to circumvent a technological measure for the sole purpose of that person performing the acts of good faith encryption research described in paragraph (2); and
>
> (B) provide the technological means to another person with whom he or she is working collaboratively for the purpose of conducting the acts of good faith encryption research described in paragraph (2) or for the purpose of having that other person verify his or her acts of good faith encryption research described in paragraph (2). 17 U.S.C. §1201 (g)(4) (2002).

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

> (A) the person lawfully obtained the encrypted copy, phonorecord, performance, or display of the published work;
>
> (B) such act is necessary to conduct such encryption research;
>
> (C) the person made a good faith effort to obtain authorization before the circumvention; and
>
> (D) such act does not constitute infringement under this title . . . .
> 17 U.S.C. §1201 (g)(2) (2002)

[36] *Reimerdes*, 111 F. Supp. 2d at 321.

the DeCSS efforts to the copyright owners; and (3) because he made no good faith effort to obtain authorization from the copyright owners.[37]

c) Security testing

Corley also argued that his actions should have been considered exempt "security testing" under Section 1201(j). However, Judge Kaplan construed Section 1201(j) to protect only the "assessing [of] a computer, computer system, or computer network, *solely* for the purpose of good faith testing, investigating, or correcting a security flaw or vulnerability, with the authorization of the owner or operator of such computer system or computer network."[38] Because DeCSS had nothing to do with testing computers, computer systems, or computer networks, the security testing exemption "ha[d] no bearing in this case,"[39] not to mention the fact that Corley had no authorization from anyone.

d) Fair use

Finally, Corley asserted that his conduct should be protected by the doctrine of fair use,[40] which limits the rights of a copyright holder by permitting others to make limited use of portions of a copyrighted work, for appropriate purposes, without incurring

[37] *Id.*
[38] *Reinerdes,* 111 F. Supp. 2d at 321 (emphasis added)..
[39] *Id.*
[40] Copyright Act, 17 U.S.C. § 107 (2002).

copyright infringement liability.[41] Judge Kaplan acknowledged that fair use "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."[42]

The Copyright Act codifies fair use in 17 U.S.C. § 107. Traditional fair use activities include conduct that might otherwise constitute an infringement of a copyright holder's exclusive Section 106 rights for purposes including "criticism, comment, news reporting, teaching…, scholarship, [and] research."[43]

As established above, to copy any part of a DVD, one must circumvent CSS. Section 107's fair use exemption provides that certain uses of copyrighted works -- uses that might otherwise be wrongful copyright infringement -- might be considered fair uses and therefore protected. Judge Kaplan, however, declined having to decide the applicability of fair use within the context of Section 1201, and simply noted that Corley was not sued for copyright infringement but 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 [DMCA]."[44] Moreover, Judge Kaplan held that fair use defenses do not apply to actions under the DMCA because "[i]f

---

[41] *Reimerdes*, 111 F. Supp. 2d at 321.
[42] *Id.* at 322.
[43] Copyright Act, 17 U.S.C. § 107. Section 107 provides that "[i]n determining whether the use made of a work in any particular case is a fair use the factors to be considered shall include - (1) the purpose and character of the use, including whether such use is of a commercial nature or is for nonprofit educational purposes; (2) the nature of the copyrighted work; (3) the amount and substantiality of the portion used in relation to the copyrighted work as a whole; and (4) the effect of the use upon the potential market for or value of the copyrighted work." No one factor is dispositive.
[44] Reimerdes, 111 F. Supp. 2d at 322.

Congress had meant the fair use defense to apply to such actions, it would have said so."[45]

Nonetheless, Judge Kaplan considered Corley's fair use argument, that DeCSS, and his posting of it, was governed by *Sony*, in which the film studios sued the Sony Corporation on the theory that its manufacturing of home video cassette recorders provided consumers with a technology that contributed to the infringing home taping of copyrighted television broadcasts.[46] Judge Kaplan rhetorically asked "whether the possibility of noninfringing fair use by someone who gains access to a protected copyrighted work through a circumvention technology distributed by [Corley] saves [Corley] from liability under Section 1201."[47]

Judge Kaplan's answer to his own question was that "[b]y prohibiting the provision of circumvention technology [in Section 1201], the DMCA fundamentally altered the landscape. A… 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. Indeed, Congress explicitly noted that Section 1201 does not incorporate *Sony*."[48]

The Second Circuit affirmed Judge Kaplan's opinion in its entirety. Circuit Judge Newman agreed with Judge Kaplan when he wrote that the fair use doctrine need not

---

[45] *Id.* Keep reading for evidence that Congress did say so.

[46] *Id.* at 323, citing Sony Corp. v. Universal City Studios, Inc., 464 U.S. 417 (1984) (establishing the rule that copyright owners have the right to control infringement-enabling technologies only when such technologies lack "substantial noninfringing uses.").

enter into this context because Corley did not "claim to be making fair use of any copyrighted materials, and nothing in the injunction prohibits [him] from making such fair use. [He is] barred from trafficking in a decryption code that enables authorized access to copyrighted materials."[49]

PART II

Discussion

There is ample reason to disagree with both Judge Kaplan and Circuit Judge Newman. A violation of Section 1201 is, for all practical purposes, an action alleging contributory copyright infringement. In contributory copyright infringement actions, defendants are permitted to argue that because the technology defendants provided to others is capable of substantial noninfringing uses, defendants should not be held liable for the direct copyright infringement of others.[50] Defendants like Corley should be permitted to assert a fair use defense in order to assert the substantial noninfringing uses of any DeCSS-like technology he is accused of using in violation of Section 1201.[51]

---

[47] *Reimerdes,* 111 F. Supp. 2d at 323-24.
[48] *Reimerdes*, 111 F. Supp. 2d at 324 n.170.
[49] Universal City Studios, Inc. v. Corley, 273 F.3d 429, 459 (2001).
[50] *Sony*, 464 U.S. 417 (1984).
[51] Even Judge Kaplan, in a footnote, let it slip that "the Sony *test* of 'capability of substantial noninfringing uses,' [is] *still operative in cases claiming contributory infringement of copyright*…" *Reimerdes*, 111 F. Supp. 2d at 324 n.170 (emphasis added). If it is recognized that *Reimerdes* is nothing more than a contributory liability action, the fair use defense should be available. Of course, there may be serious constitutional questions regarding the unavailability of the fair use defense in this context as it relates to a defendant's First Amendment rights, but answering such questions must regrettably remain the goal of further, and future, research.

Section 1201(c)(1) clearly provides that "Nothing in this section shall affect rights, remedies, limitations, or defenses to copyright infringement, *including fair use*, under this title."[52] The language is plain and unambiguous. Neither Judge Kaplan nor Circuit Judge Newman ever address Section 1201(c)(1), even though the Second Circuit has held that courts must give effect to all provisions of a statute, and "are not at liberty to construe any statute as to deny effect to any part of its language."[53]

It's erroneous for the courts to divorce Section 1201 from copyright infringement -- and thereby ignore DeCSS's substantial noninfringing uses[54] -- by merely pointing out that Corley was not sued for copyright infringement but for "offering and providing technology designed to circumvent technological measures that control access to copyrighted works…"[55] Section 1201(c)(1)'s clear terms presume that Section 1201's anti-circumvention provisions are inextricably linked with the copyright infringement context. For example, the title to Section 1201 reads, "Circumvention of *copyright* protection systems."[56] If we accept this link between Section 1201 and copyright infringement, as we should, it becomes difficult to explain why fair uses of digitally-encrypted copyrighted content are not permitted under Section 1201, while the same uses

---

[52] Copyright Act, 17 U.S.C. § 1201(c) (2002) (emphasis added).

[53] United States v. Rodriguez, 794 F.2d 24, 28 (2nd Cir. 1986) (citing Market Co. v. Hoffman, 101 U.S. 112, 115, 116 (1879)).

[54] Though this article suggests that there are several substantial noninfringing uses of DeCSS below, consider at this point the developing field of video content analysis, involving the creation of video search algorithms. DeCSS facilitates scholarly research of these algorithms that permit one to scan, index, browse and search video content much like text files, permitting large databases of video clips to be searched. For example, a researcher could enter an image they were researching and then scan a database of images to find similar images. See Appellant's Appeal Brief in *Reimerdes*, available at http://www.eff.org/IP/Video/MPAA_DVD_cases/20010119_ny_eff_appeal_brief.html . Whether or not this is a "substantial" noninfringing use is certainly debatable. But courts are able to distinguish between genuine and pretextual claims of substantial noninfringing use. Sega Enters. v. MAPHIA, 948 F. Supp. 923 (N.D. Cal. 1996).

[55] *Reimerdes*, 111 F. Supp. 2d at 322.

of unencrypted analog counterparts would be perfectly acceptable under the Copyright Act.

Put another way, if a Plaintiff claims that a defendant provided technology to circumvent the copyright protection system in violation of Section 1201, the Plaintiff has actually made a claim of contributory copyright infringement against the defendant. By providing the technology to others in violation of Section 1201(b), possibly after engaging in his own Section 1201(a) violation, the Defendant *enabled* others to violate the Plaintiff's rights under other provisions of the Copyright Act. Therefore, assuming *arguendo* that Corley did offer and provide this technology to others, the Plaintiffs' objection would be that his doing so enabled others to directly infringe the Plaintiffs' copyrights under a theory of indirect liability reminiscent of that raised in *Sony*.[57]

Copyright protection systems -- explicitly the subject of Section 1201's protective provisions -- exist to prevent copyright infringement by making it more challenging for the average consumer to access a copyright holder's encrypted copyrighted materials. Accordingly, an alleged violation of Section 1201 -- because it potentially renders the copyrighted materials protected by such anti-circumvention technology more vulnerable

---

[56] Copyright Act, 17 U.S.C. § 1201 (2002) (emphasis added).

[57] And were Section 1201 construed so as to permit the fair use defense as this article argues it should be, Plaintiffs might not suffer all that much because courts have often extended indirect liability to defendants whose dual-purpose devices contributorily infringed copyrights. *See*, *e.g.,* Fonovisa, Inc. v. Cherry Auction, Inc., 76 F.3d 259 (9th Cir. 1996) (defendant operated a flea market); RCA Records v. All-Fast Sys., Inc., 594 F. Supp. 335 (S.D.N.Y. 1984) (defendant was a commercial operator of an audiocassette duplication machine); Sega Enters. v. MAPHIA, 948 F. Supp. 923 (N.D. Cal. 1996) (defendants ran internet sites which made plaintiff's product available).

to direct infringement -- is therefore *itself* an allegation of indirect copyright infringement.[58]

In that sense, Section 1201 affords copyright holders an additional exclusive right;[59] namely, the right to prevent circumvention of copyright protection systems put in place to protect their copyrighted works (hereafter referred to as the "Protective Right"). Circumvention of copyright protection systems, and all trafficking activities associated with such circumvention, are and should be judicially regarded simply as new varieties of copyright infringement because such circumvention infringes on the copyright holder's exclusive Protective Right under Section 1201. DeCSS-like technologies are analogous to VCRs in that they may enable fair uses of copyrighted materials that might otherwise be regarded as directly infringing a copyright holder's exclusive right(s).[60]

The Circuit court avoided having to apply the fair use factors and precedent to Corley's conduct and simply affirmed Judge Kaplan's ruling, holding that "such matters are far beyond the scope of this lawsuit" because Corley does not "claim to be making fair use of any copyrighted materials."[61]

---

[58] The test for contributory liability under traditional principles of copyright law first asks, "did the defendant know or should the defendant have known about the infringing conduct?" Second, "did the defendant materially contribute to the infringing conduct?" The second inquiry usually requires actual inducing or causing of the infringing conduct, and courts may require that such participation be substantial. From the facts as they were set forth by Judge Kaplan, and to the extent that Plaintiffs could establish actual copyright infringement by a DeCSS user, it seems fairly likely that the Plaintiffs would have been able to satisfy this two-prong test for indirect liability.

[59] "Additional" in the sense that a copyright holder's exclusive rights are traditionally enumerated in Section 106 of the Copyright Act. *See* Copyright Act, 17 U.S.C. § 106 (2002).

[60] Interestingly, the parties acknowledged that they had no direct evidence of a single occasion on which any person decrypted a copyrighted motion picture with DeCSS and transmitted it over the Internet. Perhaps this is why Plaintiffs were reluctant to argue indirect liability? *Reimerdes*, 111 F. Supp. 2d at 314.

The Circuit court's comment that Corley does not "claim to be making fair use of any copyrighted materials, and nothing in the injunction prohibits [him] from making such fair use" doesn't address the fact that Corley's fair use defense arose while facing the unique circumstances of what amounted to a traditional indirect copyright infringement action cloaked within a Section 1201 action. Before the enactment of Section 1201, the Plaintiffs would have been forced to bring indirect liability actions to enjoin Corley's posting of DeCSS; actions that might have collapsed under the weight of the *Sony* precedent.[62]

Moreover, the *Reimerdes* ruling is particularly striking in light of Section 1201(c)(2)'s "Other rights, etc., not affected" clause, providing that, "Nothing in this section shall enlarge or diminish vicarious or contributory liability for copyright infringement in connection with any technology, product, service, device, component, or part thereof."[63] Construing Section 1201 in a manner precluding a fair use defense impermissibly "enlarge[s]… contributory liability for copyright infringement in connection with any technology, product, service, device, component, or part thereof"

---

[61] Universal City Studios, Inc. v. Corley, 273 F.3d at 458-59.

[62] Remember that "the Sony *test* of 'capability of substantial noninfringing uses,' [is] *still operative in cases claiming contributory infringement of copyright*…" *Reimerdes*, 111 F. Supp. 2d at 324 n.170 (emphasis added). *Sony* would work against such actions because in its light, DeCSS need only be "capable" of substantial noninfringing uses. *Sony*, 464 U.S. at 440-42. See below at Part III for some hypotheticals that explore whether or not certain proposed uses are substantial and/or noninfringing.

[63] Copyright Act, 17 U.S.C. § 1201(c)(2). Further, any expansion of indirect liability is particularly problematic if implemented without respect to (1) whether or not there was any actual infringement, and/or (2) the nature of the relationship between the alleged contributor and the alleged actual infringer. Put another way, Section 1201 could be improved simply by adding an "intent to circumvent for illegal purposes" prong, or an "intent to aid and abet copyright infringement" requirement. For example, the Vessel Hull Design Protection Act, 17 U.S.C. § 1309, requires that a disseminator of information be held liable only if he or she "induced or acted in collusion with" one who actually gains unauthorized access to a work. Under this standard, the statements of the defendants, including Corley, clearly indicate that they were, and probably did, induce the conduct of folks who used DeCSS to gain unauthorized access to Plaintiffs' copyrighted works.

because fair use is permitted as a defense to contributory liability actions under traditional copyright principles.[64] Just because Section 1201 created this new Protective Right does not mean that the Protective Right can violate the express language of Section 1201(c)(2) drafted specifically to constrain Section 1201's potential "enlarge[ment] of contributory liability." Therefore, Section 1201 does not inevitably enlarge contributory liability, or even go beyond it by creating a new form of liability.

A plaintiff's election to overlay a copyright infringement action with a Section 1201 claim should not preclude or eviscerate an otherwise potentially exculpatory fair use defense. To allow the *Reimerdes* rulings to stand for such proposition would significantly "enlarge" indirect liability -- as defendants will be deprived of the fair use defense in the contributory anti-circumvention context -- in direct contravention of Section 1201(c)(2).[65]

To deny Corley, and future defendants in this context, the fair use defense directly contravenes the intent and language of Section 1201(c) as well as the longstanding notion that "some opportunity for fair use of copyrighted materials has been thought necessary to fulfill copyright's very purpose, '[to] promote the Progress of Science and useful

[64] Sony Corp. v. Universal City Studios, Inc., 464 U.S. 417 (1984).

[65] One scholar has posed a hypothetical that I modify: A pharmaceutical company produces data indicating the safety of its new drug. Presuming that its expression of this data is copyrighted, the company releases this copyrighted information with copyright protection software to protect the data in a way so that only certain tests can be performed on this data, all of which support the safety claim, and all of which were used by the FDA to approve the drug. A skeptical scientist would be deterred from interpreting the data on his own as it might require him to circumvent the access control system and thereby contribute to the copyright infringement of others who might then check the scientist's data. Pamela Samuelson, *Anticircumvention Rules: Threat to Science*, 293 Science Magazine 2028, 2029 (2001).

Arts…."[66] Under the *Reimerdes* interpretation of Section 1201, however, copyright holders will be able to simply encrypt all of the works they distribute and thereby make it impossible for consumers to make many otherwise fair uses of any underlying copyrighted works without receiving the express authority of copyright holders, thereby eviscerating the essence of making fair uses.[67]

Permitting the fair use defense within the anti-circumvention context still provides copyright holders a remedy for the dissemination of those technologies, such as DeCSS, which they can establish lack substantial noninfringing uses. Doing so would merely require, in accordance with today's construction of the fair use doctrine, that Plaintiffs' burden of proof include a showing that the DeCSS-like technology in question is *incapable* of substantial noninfringing uses before a court imposes liability for trafficking in it.[68]

The first step in the author's test to resolve these tension would be to ask whether or not the circumvention *technology* facilitates some substantial noninfringing uses. The application of this test will not eviscerate Section 1201's ban on all such conduct. For example, Judge Kaplan never decided whether or not DeCSS facilitates substantial

---

[66] *Corley*, 273 F.3d at 458, quoting Campbell v. Acuff-Rose Music, Inc., 510 U.S. 569, 575 (1994)).

[67] An essential aspect of the making fair uses is that doing so does not require advance permission from copyright holders. Plaintiffs simply chose to release their films in digital form. Once they do, the "underpinnings of fair use and the limited nature of the copyright holder's exclusive rights require that these limits on copyright apply unless the government can sustain its heavy burden to show why these expressive uses should be banned in this new medium of expression." EFF Supplemental Letter Brief in *Reimerdes*, at http://www.eff.org/IP/Video/MPAA_DVD_cases/20010530_ny_eff_supl_brief.html .

[68] Courts should affirmatively "distinguish between circumvention aimed at getting unauthorized access to a work and circumvention aimed at making noninfringing uses of a lawfully obtained copy." Pamela Samuelson, *Intellectual Property and the Digital Economy: Why the Anti-circumvention Regulations Need to be Revised*, 14 Berkeley Tech L.J. 519, 539 (1999).

noninfringing uses. If he had done so, he probably would have found that it does not. On the other hand, one could argue that a DeCSS-like technology might facilitate substantial noninfringing uses if, for example, it allowed the removal of only a few seconds of the underlying copyrighted work, or if it permitted the lawful recording of its audio portion under the Audio Home Recording Act.[69] *Reimerdes* leaves the question unresolved.

Additionally, a redrafted Section 1201 should also ask whether or not the circumvention itself falls into the category of fair use (i.e., (1) whether or not the circumvention is for a favored purpose, (2) whether it's noncommercial, and (3) what is its effect on the market). Because Section 1201 is designed to protect copyrighted expression, circumvention of technologies that encrypt protected expression may be "fair use" under the circumstances described in Part III below. Under this analysis, Section 1201 can still restrict circumvention and the distribution of circumvention technologies that neither facilitate substantial noninfringing uses or that are not themselves fair uses.

PART III

Hypotheticals

a) Roving

[69] 17 U.S.C. § 1008 (2002).

Consider the case of Eugene, a United States citizen, who purchased a lawfully-made DVD from an authorized retailer while travelling in Spain. Because of the DVD's European regional encoding, the DVD will not play when placed in Eugene's DVD player in Los Angeles that's been factory-encoded for the United States region. At this point, Eugene can either use the DVD only when he's able to play it on a properly-encoded DVD player, perhaps only when in Spain, or, if he's sufficiently skilled, he can write or use a DeCSS-like technology to circumvent the regional encoding and enable him to view the DVD for which he already paid in his own home.

If Eugene chooses to do the latter, under Section 1201's *Reimerdes* interpretation, he will almost certainly violate Section 1201. However, this specific sort of private use activity "does no harm to the copyright owner of the DVD and is not the type of piracy-enabling activity that the DMCA's anti-circumvention provisions were intended to reach."[70] Further, application of the fair use defense under Section 107 would likely

[70] Decl. of Pamela Samuelson in Universal City Studios v. Corley, 273 F.3d 429 (2001), available at http://www.eff.org/Cases/MPAA_DVD_cases/20000503_ny_def_goldstein_samuelson_decl.html . Further, § 1201(a)(3)(A) defines the phrase "circumvent a technological measure" as allowing access to a copyrighted work "without the *authority* of the copyright owner." Copyright Act, 17 U.S.C. § 1201(a)(3)(A) (emphasis added). By purchasing the DVD in Spain, Eugene has definitively been granted the authority to access the work. Should this authority be limited to using Spain-encoded DVD players? Is this limitation reasonably clear to the average consumer who buys a DVD while abroad and then gets home to discover that it is useless on his U.S. DVD player? Did that purchaser make a contract-like promise only to render playback on Spain-encoded players? Should U.S. copyright laws and courts forced to consider them overlook these ambiguities by affirming *Reimerdes*-like interpretations of Section 1201*?* Perhaps we should defer to Congress, which considered these questions and others and indicated that "where access is authorized, the traditional defenses to copyright infringement, including fair use, would be fully applicable. So, an individual would not be able to circumvent [access control technologies] in order to gain unauthorized access to a work, but would be able to do so in order to make fair use of a work which he or she has lawfully acquired." H.R. Rep. No. 105-551, pt.1, at 18 (1998). Query whether or not the hypothetical presented above would be considered a fair use, especially where price discrimination becomes less available to the copyright holder as a result. In that sense, the fourth fair use factor -- "the effect of the use upon the potential market for or value of the copyrighted work" -- seems to resolve in favor of the copyright holder; one component of the potential market and/or value of a copyrighted work is the ability of the copyright holder to price discriminate between regions. Uses of the nature described above, if permissible, might reduce the value of the copyrighted work because a copyright owner might not

protect Eugene's conduct. Using a DeCSS-like technology to play a regionally-encoded DVD player in the privacy of one's home in another region does not infringe on any of the copyright holder's traditional Section 106 exclusive rights.[71]

The drafters of Section 1201 may have considered scenarios like this when they specifically included Section 1201(c)(1), which provided that "Nothing in this section shall affect rights, remedies, limitations, or defenses to copyright infringement, *including fair use*, under this title." Otherwise, copyright holders would be allowed to simply employ a CSS-like copyright protection mechanism in connection with their works to deny defendants the ability to raise a fair use defense in connection with activities that courts and Congress have already determined may be fair uses, especially insofar as they're related to "teaching…, scholarship, [and] research," which are explicitly referred to in Section 107. The fair use factors that consider (1) the "purpose and character of the use, including whether such use is of a commercial nature or is for nonprofit educational purposes," as well as (2) the "effect of the use upon the potential market for or value of the copyrighted work" seem to work in favor of many uses to which DeCSS can enable users to put the Plaintiffs' copyrighted works, some of which are discussed in detail in

---

sell product in poorer countries because of the risk that purchasers of the product at lower prices might circumvent the encryption for playback in regions where the same product is sold at higher prices. Nonetheless, the fourth fair use factor is at most one-fourth of the fair use inquiry. No one factor is dispositive, and the weighting of the factors varies from case to case. Finally, the factors list is only suggestive, not inclusive.

[71] Such use would likely be a private, and not a public, performance of the copyrighted work, and there's no exclusive private performance right granted to a copyright holder under the Copyright Act. Query also the effect of Section 602(a), under which absent the copyright owner's consent, importation into the United States of copies made outside of the United States is an infringement of such owner's exclusive Section 106(3) right to distribute, and is actionable under Section 501. If a copy was made inside the United States and then lawfully sold overseas, it is permissible for the copy's lawful owner to bring such copy back into the United States. Quality King Distributors, Inc. v. L'anza Research Int'l., Inc. 523 U.S. 135 (1998) (finding that "[g]iven the importance of the fair use defense to publishers of scholarly works, as well as to

this Part. For example, the "purpose and character" of many such uses is often noncommercial and nonprofit, and often has little if any effect upon the potential market for or value of the copyrighted work.

b) Reverse-engineering and cryptographic research

The anti-circumvention rules should be modified and/or interpreted so as to permit research that's currently unprotected by Section 1201's scientific or technical research exemptions.[72]

Consider the case of the computing hobbyist who is writing an article for a publication evaluating and comparing several competing CSS-like encryption technologies that protect copyrighted data on DVDs. The DMCA's reverse engineering exception applies only if the sole purpose of the reverse engineering is to achieve program interoperability and if reverse engineering is necessary to do so.[73] The hobbyist's attempts to diagram or understand the encoded encryption mechanism, even if conducted in the privacy of his own laboratory, would not qualify under this exemption and would probably violate Section 1201.[74]

---

publishers of periodicals, it is difficult to believe that Congress intended to impose an absolute ban on the importation of all such works containing any copying of material protected by a United States copyright.").

[72] See *supra* at note 32.

[73] Copyright Act, 17 U.S.C. § 1201(f)(1).

[74] Such attempts might constitute a violation of Section 1201 specifically because they're aimed not at achieving interoperability but at gaining knowledge. Even where the hobbyist had both goals in mind would still violate Section 1201 because interoperability must be the "sole" purpose of the reverse engineering. And what about inchoate reverse engineering, or experiments that stop short of reverse engineering but which get pretty close?

Further, the hobbyist could not share any information gained from such activities with others, except for the purpose of enabling program interoperability.[75] Accordingly, situations like the one described above would never qualify under this exception because a DVD's copyrighted material is not a program, it is *data*, and data-to-program interoperability[76] is not covered by the exemption.[77]

Likewise, the cryptographic research[78] exemption, for example, may apply only if the defendant is employed or has been specifically trained as a cryptographer.[79] Cryptography, however, is a field unlike molecular biology or even formal computer science; its practitioners are often occasional hobbyists,[80] or what others would describe as "amateurs."[81]

Further, the cryptographic exemption requires a person engaged in research[82] to prove the necessity of such research. However, as suggested above, a person might just

---

[75] Copyright Act, 17 U.S.C. § 1201(f)(3) ("The information acquired through the acts permitted under [this subsection] may be available to others if the [information sharer] provides such information or means *solely* for the purpose of enabling interoperability of an independently created computer program with other programs…") (emphasis added). Is anything ever done solely with any particular purpose? What about when information is shared for no purpose but the expansion of the recipient's knowledge?

[76] Or, more accurately, "compatibility."

[77] Pamela Samuelson, *Anticircumvention Rules: Threat to Science*, 293 Science Magazine 2028, 2029 (2001).

[78] It is somewhat amusing to note how cryptic the cryptographic exemption itself is.

[79] Copyright Act, 17 U.S.C. § 1201(g)(3)(B).

[80] One commentator has suggested that cryptography is not a "members only" club; anyone with the motivation to learn and the ability to contribute is welcome. Bruce Schneier, *Self-Study Course in Block Cipher Cryptanalysis*, 24 Cryptologia 1, 18 (2000).

[81] Pamela Samuelson, *Anticircumvention Rules: Threat to Science*, 293 Science Magazine 2028 (2001).

[82] Defined as "activities necessary to identify and analyze flaws and vulnerabilities of encryption technologies applied to copyrighted works, if these activities are conducted to advance the state of knowledge in the field of encryption technology or to assist in the development of encryption products…" Copyright Act, 17 U.S.C. § 1201(g)(1)(A). Where's the boundary between "research" and that which is prohibited under Section 1201? Is it still "research" if a person writes down the flaw and then writes a computer program to test it in a safe digital environment against CSS-protected works? One could argue that this test would not be "necessary to identify and analyze flaws and vulnerabilities of encryption

be trying to enhance his or her understanding of how an existing technology works, with, without, or perhaps before having an eye towards advancing the field.

Section 1201 could be redrafted to take these hypotheticals into account and provide a way for students and those entering the field to lawfully conduct their own education and promote future contributions to the field by learning through experimentation. For example, Section 1201 could explicitly exempt uses that it might otherwise ban using language similar to Section 110's teaching exemption.[83] To determine what object code is doing, for example, some computer programmers use programming tools (sometimes called disassemblers or decompilers), to translate object code back into source code that can readily be studied by beginners.[84] None of this is clearly protected conduct under Section 1201, and it should be.[85]

---

technologies" because any such flaws were already identified. More importantly, how is anyone to know in advance what's *verboten*?

[83] Copyright Act, 17 U.S.C. § 110 (2002). Section 110 limits the exclusive performance and display rights by protecting the "performance or display of a work by instructors or pupils in the course of face-to-face teaching activities of a nonprofit educational institution, in a classroom or similar place devoted to instruction." *Id*. at § 110(a)(1). In the anti-circumvention context, Section 1201 should expressly protect circumvention "by [those] engaged in the course of noncommercial research or educational activities." This might indeed extend beyond classroom teaching to research and/or educational websites and periodicals.

[84] One cryptographer website has noted that, "[t]he only way to learn cryptanalysis is through practice. A student simply has to break algorithm after algorithm, inventing new techniques and modifying existing ones. Reading others' cryptanalysis results helps, but there is no substitute for experience." Bruce Schneier, *Self-Study Course in Block Cipher Cryptanalysis,* 24 Cryptologial, 18 (2000) *available at* http://www.counterpane.com/cryptanalysis.pdf .

[85] This does not undermine Section 1201 because Section 1201 is supposed to preserve fair use, and educational uses are favored under fair use analysis. If, for example, a programmer simply posts object code on his website and claims to merely be sharing his ideas, he still must withstand the scrutiny of whether or not his technology has substantial noninfringing uses. If it does not, he will be in trouble. If it does, but if it contributes to the direct infringement of another in satisfaction of the indirect liability test, Plaintiffs will still be able to remedy those wrongs. But a Plaintiff should not simply be permitted to point to Section 1201 and contend that a defendant is in violation of it without reference to fair use and contributory liability, neither of which are to have been "enlarge[d]" by Section 1201. Copyright Act, 17 U.S.C. § 1201(c)(1),(2) (2002).

Consider another hypothetical situation: a copyright holder authorizes the creation of a very well-crafted algorithm to protect and restrict access to his copyrighted materials. This algorithm would then *itself* be locked away from use or even understanding by others under Section 1201 to the extent that learning about the algorithm requires circumventing any technology used to encrypt it. If successful, all of the beneficial ideas of this breakthrough method or procedure would inure only to the copyright holder.[86] Other computer programmers would be barred from even attempting to learn how this authentication or encryption procedure works or how/if it can be adapted to another purpose. This is likely not the intent of Section 1201.[87]

Cryptographers and computer programmers tend to engage in their trade during and after a process of exchanging ideas in computer code with one another. Section 1201's encryption research exemption strictly limits the ability of these people from communicating with one another with respect to all of the research situations I've outlined.[88] All of this behavior would likely be prohibited by the anti-circumvention rules as they're set forth in Section 1201 and interpreted in *Reimerdes*.[89] Further, even receipt of authority from the copyright owner of a particular work protected by the

[86] Under traditional copyright principles, copyright laws protect only expression, not ideas. This notion has been codified in the Copyright Act, 17 U.S.C. § 102(b) (2001): "In no case does copyright protection for an original work of authorship extend to any idea, procedure, process, system, method of operation, concept, principle, or discovery, regardless of the form in which it is described, explained, illustrated, or embodied in such work." Of course, trade secret doctrine and case law still exist to protect unlawful conduct thereof.

[87] It is possible, but unlikely, especially because the very title of the act evidences a primary interest in preventing the infringement of the encrypted copyrighted work. Moreover, if we take Section 1201 as it was interpreted in *Reimerdes*,if a content provider placed a copyrighted work in an electronic database, Section 1201 would render it unlawful to circumvent technology controlling access to that database even if the database contains mostly public domain works. Neil Weinstock Netanel, *Locating Copyright Within the First Amendment Skein*, 54 Stan. L. Rev. 1, 75 (2001).

[88] Again, the issue of the First Amendment arises, and remains beyond the scope of this paper.

encryption technology that is the subject of analysis might still constitute "offer[ing] to the public [or] provid[ing]" a "technology" for circumventing access or copy controls on a *different* work encrypted by the same method because the lessons learned from one may be applied to the other.[90]

Another potential conflict between the anti-circumvention rules and fair use is illustrated by the following hypothetical: a university professor lawfully purchases a digitized -- but encrypted -- multi-volume index to a very large body of scholarly work. The index is searchable using whatever protocols the copyright holder has established, but the search characteristics are limited in function.[91]

If the professor wants to employ his own search methodologies, either by writing or using code to bypass the in-built search function,[92] the professor risks violating Section 1201 because the index data has been encrypted using a CSS-like copyright protection technology. The uses to which the professor would have put the encrypted data would probably have been fair uses under pre-Section 1201 copyright principles. Still, the professor would likely be prevented from accessing this information in this way under Section 1201(a)(1)(A), which states the blanket prohibition that "[n]o person shall circumvent a technological measure that effectively controls access to a work protected under this title."

---

[89] Remember that to the extent such behavior contributes to direct copyright infringement, Plaintiffs are always able to bring indirect liability actions against such actors under contributory liability theories.
[90] Copyright Act, 17 U.S.C. § 1201(a)(2), (b)(1).
[91] This issue was raised in the *Reimerdes'* Educators' Amici Brief, available at http://www.eff.org/IP/Video/MPAA_DVD_cases/20010126_ny_edu_amicus.html .
[92] Perhaps the professor is studying the various strengths and weaknesses of common search feature codes themselves!

One could argue that a copyright owner should be permitted to determine how a body of data that such owner has expressively arranged should be searched. However, the stronger argument is that once consumers have purchased a body of information, devising a new way to search that information, especially when searched for private purposes only, should be protected because consumers would be permitted to do just this by cutting the body of information up into small pieces and organizing them alphabetically or in some other order -- why make them engage in this sort of waste?

Just as there is nothing in a copyright that requires a person to a read a book from front to back, there should be nothing in a copyright that requires him or her to search through that book using only its table of contents. If one decides to wear special eyeglasses designed to permit reading only the word "fancy" as it appears in the book, especially where one is researching the uses of the word "fancy" in literature and the book is not otherwise equipped with a mechanism to provide her with this data automatically, there should be no copyright objection to her devising a program aimed at this end. The data, the facts, are all in the lawfully-purchased copy; should we permit the copyright holder to restrict access to these facts as he determines? Circumvention that helps facilitate uses of facts should be at least as protected as circumvention that facilitates fair uses of expression.[93]

[93] The second and third fair use factors would enter into this analysis here because the amount and substantiality of the work used is often minimal (e.g., the professor's in-class use). This is especially so with copyrighted works of a nature particularly suited for instruction.

Yet another hypothetical conflict is illustrated by the beginning computer programmer who has been assigned by his professor to devise an encryption algorithm to protect the data on the programmer's personal computer. The programmer's computer, however, contains material copyrighted by others, including, for example, songs lawfully-transferred from one of the programmer's CDs, and the text of various commercially-available news articles.

One day while in the midst of composing a particularly tricky section of code, the programmer's encryption algorithm corrupts commercial encryption software associated with some of the copyrighted material lawfully resident on the programmer's computer. Apparently, both of the encryption technologies access a third piece of code to run properly with the programmer's operating system. Immediately, the programmer's computer locks up and will not permit him to access his hard drive. The student takes his computer to his professor who might be able to help the student separate the warring algorithms, permitting him to access the materials on his hard drive. The professor quickly isolates the conflict-causing code sections, breaks the algorithm that caused the conflict, and hands the computer back to the student.

There's nothing in Section 1201 that exempts the professor's conduct from constituting a violation of Section 1201(a)(1)(A). The professor, if successful, would have circumvented a technological measure that effectively controls access to a work protected under the Copyright Act (the songs, for example). Under traditional copyright principles, however, this would be a fair use. For example, the purpose or character of

the circumvention was for nonprofit educational activities, a favored use, and there's also likely to be no effect on the market for those materials under these facts. To the extent that the CSS-like technologies were circumvented, such circumvention was not conducted to use any protected copyrighted materials at all. The other two fair use factors are therefore inapplicable. Finally, under *Sony* a copyright holder would be permitted to restrain the sale of professor's potentially infringement-enabling technology -- currently forbidden under Section 1201(b) -- only when it could be proved incapable of substantial noninfringing uses.[94]

c) Expression and education

Though a discussion here of the possible collision of the First Amendment and the *Reimerdes* facts could potentially open a can of worms, the *Reimerdes* decisions and their courts' construction of Section 1201 do pose significant practical obstacles to the freedom of the press.

Imagine that in the fall of 1998, an Enron file-clerk gets wind of some accounting irregularities that suggest that high-level Enron executives have possibly misrepresented the corporation's revenues, assets, and liabilities. The file-clerk brings this to the attention of a senior vice-president who tells her to keep it quiet or she'll lose her job. The public disclosure of this information to the media, however, could potentially prevent the loss of millions of dollars in pension packages, and timely attention to this matter may

[94] Provided, of course, that the professor or any similarly-situated defendant could prove that such technology is an article of commerce. Sony, 464 U.S. at 441-48.

help protect the jobs of many lower-level Enron employees, including that of the potential whistle-blower, by drawing government attention to what could become a disaster long before it actually is one.

The file-clerk comes across a computer disk that she knows contains this data in support of her suspicions, but the data is protected by CSS-like software enabling only authorized Enron terminals to access the data.

Presuming the legitimate copyrightability of the data by Enron, a publicly-held company, the file-clerk, or a journalist to whom the file-clerk gives the disk, or any of their agents, may need to decrypt the protection software to view the underlying information. Under *Reimerdes,* this conduct, clearly in the public interest, would likely violate Section 1201 and may subject the whistle-blower to a successful Section 1201 action if she's barred from asserting the fair use defense. Though the file-clerk would be subject to all sorts of criminal and civil liabilities for theft of corporate property, trade secrets, embezzlement, and/or conversion, that is no excuse on its own for adding copyright liability to the book that the courts are going to throw at her. Electronic data such as that encrypted on the disk is unlike ordinary or traditional property; its use will not be one that infringes on the copyright holder's exclusive rights to remuneration from his protected expression.

By simply electing to protect its sensitive data with a copyright protection system like CSS, companies like Enron could further deter whistle-blowing and diminish

corporate accountability in derogation of the rights and interests of their employees and shareholders. The Enron employee could find herself with no possible way to save her own job without being subjecting to a Section 1201 action (in addition to the legion of other actions to which she'd reasonably be subject).

In another context, a professor might need to access a film only available on DVD for use in a compiled presentation of several clips to illustrate a lesson during a class. Section 1201 provides no protection for this sort of harmless educational use.[95] For pedagogical efficiency purposes, professors will often make "mix" tapes of various copyrighted media to insert and play from start to finish so as to minimize time spent changing between source materials. As suggested above in the other hypothetical involving a professor, this too is a favored use by virtue of its connection with in-class education.[96] Consider also the above-mentioned hypothetical involving a content provider who placed a copyrighted work in an electronic database. Section 1201 would render it unlawful to circumvent technology controlling access to that database even if the database contains mostly public domain works.[97]

---

[95] At least one professor, Princeton's Peter Ramadge, has noted that his research in the field of video content analysis has been stymied by lack of access to high quality digital video. See Educators' Amici Brief in *Reimerdes*, available at http://www.eff.org/IP/Video/MPAA_DVD_cases/20010126_ny_edu_amicus.html . Professor Ramadge was trying to develop video search engines to scan and index video files on the Internet. For example, someone with an image of a laptop could search a database of video clips for similar images. Professor Ramadge's research requires access to digital video content for it to be updated with new movies only out on DVD. Such use should qualify as fair use of underlying ideas, especially when it's for research and scholarship. DeCSS-like technologies may enable fair uses of copyrighted materials encrypted on a DVD.

[96] Copyright Act, 17 U.S.C § 110 (2002).

[97] *supra*, at note 85.

In the future, diminished protection for this sort of conduct might come at a great cost for students of film and television who might be limited to watching clips from older analog sources that don't employ the CSS-like technologies that prevent them from being used or compiled by instructors. Moreover, Section 1201 will serve to make professors go through the motions of switching between DVDs that detracts from the learning process and increases the length of time between segments to be compared. When films begin to be released only on DVD, much like many recordings are released only on CD today, these tensions may become exacerbated in many instructional contexts. This is especially true if Section 1201 continues to be interpreted so as to enable copyright holders to effectively to control access to content as well as the uses that fall within their exclusive Section 106 rights.

More generally, the sorts of encryption technologies used by copyright holders might not be truly "impossible," but as the hypothetical situation above suggests, copyright holders might be able to deter such uses by making them so impractical.

Conclusion

As intellectual property doctrines such as trademark and copyright increasingly begin to collide with the legal traditions associated with fair use and the First Amendment, lawyers and judges will be forced to define the extent to which these doctrines and legal traditions can coexist and provide adequate protection to both potential plaintiffs and defendants. Perhaps this collision will result in an ebb and flow of

advantage over a number of years, with *Reimerdes*-like decisions vesting precedential authority in copyright holders only until new technologies and/or Supreme Court reviews render such decisions either of limited value or altogether invalid.

The natural tendency for information is to escape from that which constrains it because those who use information rarely do so for themselves alone. Before personal computers, photocopying threatened copyright, and before photocopying the spoken word permitted those who had not purchased a book to learn of and from its contents, its ideas, without the permission of the copyright owner. Once information has been set forth in a fixed medium, the tendency is for it to be shared with others, whether by spoken word, a photocopy-like reproduction, or digital transmission. Frameworks established to constrain this tendency often collide with the essential purpose of memorializing that information in the first place: communication. On the other hand, there is meaningful value in maintaining incentives for producers to create new works. Section 1201's interpretation in *Reimerdes* strikes this balance too strongly in favor of copyright holders, but this imbalance can be remedied by the proposals made herein.

The challenge for the developers of emerging technologies will be to accommodate the interests of content-producers in protecting their investments with the natural tendency of information to escape from that which may constrain it in furtherance of communication. Of course, this tendency needs to be kept in check so as to protect the equally natural desire to protect the value of created works. In writing this paper, for example, this author came across two technologies that have found a way to accomplish

at least some of what Section 1201 may have been seeking to avoid without risking its violation.[98]

Fair use may remain the doctrine by which the average person's right to make fair use of another's copyrighted intellectual property retains at least a threshold level of protection. Alternatively, courts and Congress may decide that fair use should become a thing of the past, relevant only in those halcyon days before the truly digital age that brought about its demise. Perhaps our future will be one in which few uses of another's copyrighted or otherwise-protected intellectually property will be "fair," and we may all be the better for it. Until then, however, copyright holders should not be permitted to use one protective copyright doctrine to eviscerate the protections long-afforded by another.

[98] ClearPlay and Movie Mask are two very similar technologies currently available to people who want to edit a commercially-available DVD before their children watch it. The technologically is painfully simple: the user downloads a program that carefully instructs a computer's DVD player to either automatically insert graphics that obscure displays of nudity, or simply to automatically fast-forward scenes containing nudity, violence, or profanity all together. These technologies do not circumvent any anti-circumvention technology at all; in fact, they access the underlying copyrighted material precisely as it is stored on the DVD itself. However, the performance that's ultimately rendered does not reflect the character of the performance as the copyright holder encoded it to the DVD. To the extent that one of Section 1201's purposes was to protect copyrighted materials from modification by someone other than the copyright holder by encrypting those materials and constraining one's access to them, these two technologies seem to accomplish that end without violating Section 1201. Visit http://www.clearplay.com , and http://www.moviemask.com to check these technologies out for yourself.