CIRCUMVENTING AUTHORITY: LOOPHOLES IN THE DMCA'S ACCESS CONTROLS

ADAM L. RUCKER[1]

ABSTRACT

In a world where digital pirates freely roam the internet, seemingly plundering at will, the providers of digital content must find a way to protect their valuable assets. Digital fences afford that protection—but not very well. Fortunately (for content owners), 17 U.S.C. § 1201, passed as part of the Digital Millennium Copyright Act of 1998, was designed to fill the numerous gaps in those fences by forbidding activities designed to circumvent them. In its present state, however, § 1201 does not adequately serve that purpose. Substantial flaws in the language of the statute render it virtually powerless to thwart piracy. If § 1201 is to fulfill its intended role (without the need for creative judicial interpretation), it must be amended to rectify the discrepancies between Congress' supposed intent and the language it chose.

INTRODUCTION

¶1 In response to the spectacular technological advances that were ushered in as part of the "digital millennium," Congress felt the need to pass legislation that would help ensure U.S. dominance in the global marketplace.[2] Realizing that today's media is, by virtue of its digital nature, more readily pirated than its analog predecessors, Congress focused its attention on technological measures designed to prevent unauthorized access to digital content.[3] As part of the Digital Millennium Copyright Act ("DMCA"),[4] Congress passed legislation making it illegal to circumvent the "digital barbed wire" content owners had begun attaching to their copyrighted works.

¶2 The idea was simple: unless it is illegal to break through the digital fence, one resourceful hacker could potentially thwart an entire protection scheme by distributing the virtual wire cutters to the public with impunity. By attaching legal sanctions to both the act of cutting the wires *and*

---

[1] J.D. candidate, Duke University School of Law, 2009; M.S. Neuroscience, University of Wisconsin-Madison, 2005; B.S. Agricultural Biotechnology & Biology, University of Kentucky, 2002.

[2] *See* S. REP. NO. 105-190, at 1 (1998).

[3] *See* Universal City Studios, Inc. v. Reimerdes, 111 F. Supp. 2d 294, 318 (S.D.N.Y. 2000), *aff'd.*, Universal City Studios, Inc. v. Corley, 273 F.3d 429 (2d Cir. 2001).

[4] Pub. L. No. 105-304, 112 Stat. 2860 (1998).

supplying the wire cutters, Congress hoped to ward off potential pirates and provide an extra incentive for content owners to use technological access controls.[5]

¶3 However simple the idea, it has proven difficult to implement. The statutory language of the DMCA's anti-circumvention provisions currently contains two major loopholes—both are found within the statutory definitions.[6] Thus far, only one court has taken the opportunity to present an in-depth textual analysis of either of these key provisions.[7] However, given the controversy surrounding the DMCA's access controls, Congress would be wise to pay these loopholes strict attention—for their shrewd opponents (the pirates) surely will.

I. THE BIRTH OF COPYRIGHT ACCESS CONTROLS

¶4 Depending on one's personal vision of the appropriate level of copyright protection and the propriety of policy-laundering, the way in which the DMCA was implemented is either brilliant or ludicrous.

¶5 Shortly after his inauguration in 1992, President Bill Clinton appointed an "Information Infrastructure Task Force" to help develop his administration's policy regarding the Information Superhighway.[8] Bruce A. Lehman, the newly-appointed Assistant Secretary of Commerce and Commissioner of Patents and Trademarks, chaired the task force's intellectual property Working Group.[9] Commissioner Lehman, who had previously served as an attorney for the computer software industry,[10] quickly began working to provide copyright holders with "as much legal control as possible over digital content."[11] When his efforts to push legislation through Congress were met by strong opposition from groups such as the Digital Future Coalition,[12] Lehman turned to the international community for (covert) assistance.[13] "He focused his attention on getting his agenda adopted by the World Intellectual Property Organization

---

[5] *See* S. REP. NO. 105-190, at 8.
[6] *See infra* pp. 12–19.
[7] I.M.S. Inquiry Mgmt. Sys., Ltd. v. Berkshire Info. Sys., Inc., 307 F. Supp. 2d 521, 531–33 (S.D.N.Y. 2004) (holding that the unauthorized use of a legitimate password does not amount to "circumvention" under § 1201).
[8] JESSICA LITMAN, DIGITAL COPYRIGHT 90 (2001).
[9] *Id.*
[10] *Id.*
[11] Bill D. Herman & Oscar H. Gandy, Jr., *Catch 1201: A Legislative History and Content Analysis of the DMCA Exemption Proceedings*, 24 CARDOZO ARTS & ENT. L.J. 121, 130 (2006).
[12] LITMAN, supra note 8, at 124–25.
[13] *Id.* at 129.

("WIPO") member nations, reasoning that when the United States signed the treaty, Congress would be obliged to adopt implementing legislation."[14]

¶6 Adopted in 1996, the WIPO Copyright Treaty[15] requires member countries to implement "adequate legal protection and effective legal remedies against the circumvention of effective technological measures that are used by authors in connection with the exercise of their [copy]rights."[16] Even though then-current U.S. law arguably met the standards adopted by the WIPO Copyright Treaty, "Congress used the Treaty as an excuse to implement a much more sweeping ban on circumvention." [17] The result was 17 U.S.C. § 1201.[18]

II. A (VERY) BRIEF LEGISLATIVE HISTORY

¶7 At the dawn of the digital millennium, Congress realized that if the law was to keep pace with the spectacular technological advances of society, it "must adapt in order to make digital networks safe places to disseminate and exploit copyrighted materials."[19] Congress hailed § 1201 as an avenue for "quickly and conveniently" exposing the internet generation to "the movies, music, software, and literary works that are the fruit of American creative genius."[20] It was designed to provide the protection and legal framework necessary to establish American dominance in the "global digital on-line marketplace for copyrighted works."[21]

¶8 "The copyright industries are one of America[']s largest and fastest growing economic assets."[22] They "contribute more to the U.S. economy and employ more workers than any single manufacturing sector, including chemicals, industrial equipment, electronics, food processing, textiles and apparel, and aircraft."[23] Indeed, in 1996, the copyright industries accounted for more foreign sales and exports than any other major industry sector.[24]

¶9 The anti-circumvention provisions of § 1201 were intended to "encourage[] technological solutions" to piracy by providing legal sanctions

---

[14] *Id.*
[15] Wipo Copyright Treaty (WCT) (1996) with the Agreed Statements of the Diplomatic Conference That Adopted the Treaty, Apr. 12, 1997, S. TREATY DOC. NO. 105-17, 2186 U.N.T.S. 152 [hereinafter WIPO Copyright Treaty].
[16] *Id.* at art. 11.
[17] Herman & Gandy, supra note 11, at 131.
[18] *Id.*
[19] S. REP. NO. 105-190, at 1 (1998).
[20] *Id.* at 6.
[21] *See id.* at 1.
[22] *Id.* at 7.
[23] *Id.*
[24] *Id.*

against the circumvention of such technology.[25] Realizing that "what may be encrypted or scrambled often may be decrypted or unscrambled," Congress thought it necessary to provide an alternate form of protection to those willing to invest in (and implement) "effective" technological measures.[26] Section 1201 "does not mandate the adoption of any . . . technological protection;" it merely "takes those technological measures that win adoption because of their efficacy and confers [statutory] protection on them."[27] If, as Congress suggested, the circumvention of a technological measure designed to protect a copyrighted work truly is "the electronic equivalent of breaking into a locked room in order to obtain a copy of a book," providing a legal remedy if the lock fails seems entirely reasonable and appropriate.[28]

III. THE (UN)COPYRIGHT

¶10 Section 1201's presence in Title 17 of the United States Code belies the fact that it is not truly a copyright law.[29] Section 1201 neither confers nor modifies *any* property rights.[30] Instead, the statute merely sanctions a new method of protecting copyrighted works—technological access controls.[31] Perhaps surprisingly, § 1201 does not even reserve its benefits for copyright owners;[32] it affords the same protection to all persons, regardless of whether they actually own the copyrights to the work they are protecting.[33]

---

[25] *Id.* at 8. Citing portions of the Copyright and Communications Acts—provisions 17 U.S.C. § 1002(c) and 47 U.S.C. § 605(e)(4)—the Senate Judiciary Committee noted that such anti-circumvention is not unprecedented. *Id.*

[26] Universal City Studios, Inc. v. Reimerdes, 111 F. Supp. 2d 294, 318 (S.D.N.Y. 2000), *aff'd.*, Universal City Studios, Inc. v. Corley, 273 F.3d 429 (2d Cir. 2001).

[27] DAVID NIMMER, NIMMER ON COPYRIGHT § 12A.03 (2007).

[28] *See* H.R. REP. NO. 105-551(I), at 17 (1998).

[29] *See* Chamberlain Group, Inc. v. Skylink Technologies, Inc., 381 F.3d 1178, 1192–94 (Fed. Cir. 2004).

[30] *Id.* at 1192.

[31] *Id.* at 1194.

[32] 17 U.S.C. § 1203 (2006) ("Any person injured by a violation of section 1201 . . . may bring a civil action in an appropriate United States district court for such violation.").

[33] The provisions of § 1201 directly address "work[s] protected under [Title 17]," but do not require that the technological measures designed to protect those works be put in place by the copyright owner. As such, the source of the technological measure may be injured by an act of circumvention despite the fact that his digital fence is designed to prohibit only the unauthorized access of a protected work for which he does not hold the copyright.

¶11 The curious nature of § 1201 emanates from the protection it affords: access control. Section 1201(a)(1) is designed to prohibit individuals from accessing copyrighted works via circumvention of technological measures designed to protect those works.[34] Section 1201(a)(2), in contrast, prohibits trafficking in "any technology, product, service, device, component, or part thereof" that 1) is "primarily designed… for the purpose of circumventing a technological measure that effectively controls access to a [copyrighted] work,"[35] 2) "has only a limited commercially significant purpose or use other than to circumvent" an effective technological measure,[36] or 3) "is marketed . . . for use in circumventing" an effective technological measure.[37]

¶12 It is noteworthy that one can easily run afoul of § 1201 without infringing any of the traditional rights enjoyed by copyright owners.[38] One need not make illegal copies or publicly display the copyrighted work to violate § 1201. In fact, such acts clearly do *not* violate § 1201. Section 1201 is concerned only with how the work is accessed, not what is done to/with the copyrighted work after access is attained.

A. Impenetrable Armor?

¶13 In the nine years since its passage, § 1201 has been used numerous times to successfully thwart those seeking to facilitate unauthorized access to copyrighted works.[39] Not surprisingly, the major industry players— motion picture studios and the music recording industry— have been at the epicenter of § 1201 litigation. They have faired very well; thus far, the courts who have interpreted the statute have given almost perfect deference to the will (though not necessarily the words) of Congress.[40]

¶14 In *Universal City Studios, Inc. v. Reimerdes*, for example, eight major motion picture studios successfully employed the DMCA against

---

[34] *See* STAFF OF H. COMM. ON THE JUDICIARY, 105TH CONG., SECTION-BY-SECTION ANALYSIS OF H.R. 2281 AS PASSED BY THE UNITED STATES HOUSE OF REPRESENTATIVES ON AUGUST 4, 1998, at 5 (Comm. Print, Serial No. 6, 1998) [hereinafter ANALYSIS OF H.R. 2281].
[35] 17 U.S.C. § 1201(a)(2)(A) (2006).
[36] 17 U.S.C. § 1201(a)(2)(B) (2006).
[37] 17 U.S.C. § 1201(a)(2)(C) (2006).
[38] *See* 17 U.S.C. § 1201(c)(1) (2006) ("Nothing in this section shall affect rights, remedies, limitations, or defenses to copyright infringement, including fair use, under this title.").
[39] *See, e.g.*, Universal City Studios, Inc. v. Reimerdes, 111 F. Supp. 2d 294 (S.D.N.Y. 2000), *aff'd.*, Universal City Studios, Inc. v. Corley, 273 F.3d 429 (2d Cir. 2001).
[40] *See id.* at 318 (citing to various House Committee reports regarding the purpose of § 1201).

defendants who posted DVD decrypting software on their website.[41] *Reimerdes* is a prime example of the type of analysis that is usually applied to § 1201 cases. As such, it is worthwhile to delve into the court's rationale.

¶15 Unlike traditional, analog video, digital video can easily be replicated without appreciable degradation.[42] For obvious reasons, the movie studios were apprehensive about the threat of piracy when they developed DVD technology.[43] So, in the mid-1990s, the studios got together with the consumer electronics industry and formulated a plan to protect their investment.[44] Their partnership gave birth to the Content Scramble System ("CSS").[45]

¶16 CSS is a system whereby the sound and graphic files that constitute a DVD motion picture are encrypted according to a defined algorithm.[46] "A CSS-protected DVD can be decrypted by an appropriate decryption algorithm that employs a series of keys stored on the DVD and the DVD player."[47] The technology for making CSS-compliant DVD players was licensed to consumer electronics manufacturers "subject to strict security requirements," which were designed to ensure that the keys to this newly-minted content lockbox were kept hidden from the public.[48]

¶17 Despite their meager efforts, the movie studios were unable to secure the digital content contained within their DVDs. In the fall of 1999, a Norwegian teenager named Jon Johansen successfully cracked the encryption scheme.[49] By reverse engineering a licensed DVD player, Mr. Johansen uncovered both the CSS encryption algorithm and the keys needed to operate the lock.[50]

¶18 Johansen and his colleagues utilized the information they gleaned from the DVD player to create a computer program capable of decrypting and "ripping" encrypted DVDs, thereby allowing them to both play the DVDs on non-compliant computers and copy the decrypted files to computer hard drives.[51] Mr. Johansen then shared his computer program with the world by posting the executable code on his personal Internet web

---

[41] *Id.*
[42] *Id.* at 309.
[43] *See id.*
[44] *Id.*
[45] *Id.*
[46] *Id.* at 309-10.
[47] *Id.* at 310.
[48] *Id.*
[49] *Id.* at 311.
[50] *Id.*
[51] *Id.*

site.[52] Since that time, his program "has become widely available on the Internet, where hundreds of sites now purport to offer the software for download."[53]

¶19 Mr. Johansen's program, DeCSS, lies at the heart of *Reimerdes*. The primary defendant, Eric Corley, is a self-proclaimed cyber revolutionary.[54] In addition to publishing a magazine called *2600: The Hacker Quarterly*, Corley also operates a website[55] dedicated to various hacker-related interests.[56] When Corley's web site began to offer direct downloads of DeCSS, as well as links to "mirror" sites where visitors could download the decryption software, the motion picture industry sought a legal remedy.[57]

¶20 The anti-circumvention provisions of § 1201 provided the studios with ammunition. Although Corley was not himself accused of circumventing the studios' access controls,[58] he had almost certainly violated § 1201(a)(2) by trafficking in circumvention technology.[59] Mr. Corley, and those like him, were exactly the type of pirates that § 1201 was designed to capture.

¶21 The district court first found that DeCSS constitutes "technology" within the meaning of § 1201(a)(2).[60] Further, the court held that DeCSS was primarily designed to circumvent CSS.[61] Indeed, as the court noted, "that is all it does."[62] Accordingly, Corley's posting of DeCSS was found to be a *prima facie* violation of §§ 1201(a)(2)(A) and 1201(a)(2)(B).[63]

¶22 DeCSS was clearly designed to circumvent the technological measure protecting CSS-encrypted digital video. That, however, is not

---

[52] *Id.*
[53] *Id.*
[54] *See id.* at 308 ("Corley is viewed as a leader of the computer hacker community and goes by the name Emmanuel Goldstein, after the leader of the underground in George Orwell's classic, *1984*.").
[55] 2600: The Hacker Quarterly, http://www.2600.com (last visited Jan. 21, 2009).
[56] *Reimerdes*, 111 F. Supp. 2d at 308.
[57] *Id.* at 312.
[58] *Id.* at 316.
[59] *See id.* at 312, 317 (stating that Corley "offered and provided and, absent a court order, would continue to offer and provide DeCSS to the public by making it available for download on the 2600.com web site").
[60] *Id.* at 317.
[61] *Id.* at 318.
[62] *Id.* Based upon the court's finding, DeCSS must have no "commercially significant purpose or use other than to circumvent a technological measure." 17 U.S.C. § 1201(a)(2)(B) (2006).
[63] *Reimerdes*, 111 F. Supp. 2d at 319.

enough to satisfy § 1201. The anti-circumvention provisions of § 1201 apply only to the circumvention of technological measures that "effectively control[] access to a work protected under [Title 17]."[64]

¶23 At trial, Corley and his fellow defendants argued that CSS, "which is based on a 40-bit encryption key, is a weak cipher that does not 'effectively control' access to [the studios'] copyrighted works."[65] Corley's argument was based on a marked misreading of (or complete failure to read) § 1201. Corley's contention—that successful circumvention proves that the technological measure was not effective—is, as the district court aptly remarked, "indefensible."[66] "The mere circumstance that [a] defendant has deactivated the subject technology cannot mean that the technology fails to offer 'effective control' as otherwise the statute would be rendered nonsensical."[67]

¶24 In holding that CSS "effectively controls" access to the copyrighted work,[68] the court purported to focus its attention on the statutory definition provided in § 1201(a)(3).[69] Section 1201(a)(3)(B) stipulates that "effective" control requires the "authority of the copyright owner." Without the authority of the studios, it reasoned, Corley could not have "legally gain[ed] access to the keys" needed to decrypt the CSS algorithm.[70] Ergo, CSS must be "effective" because the copyright owner's permission is required in order to properly operate the system.

¶25 "This view," the court declared, "is confirmed by the legislative history."[71] The House Judiciary Committee's section-by-section analysis of § 1201 states that "[t]he practical, commonsense approach taken by [the statute] is that if, in the ordinary course of its operation, a technology actually works in the defined ways to control access . . . then the 'effectiveness' test is met, and the prohibitions of the statute are applicable."[72] The "ordinary course of operation" for CSS, the court determined, is confined to those instances "when DeCSS or some other decryption program is not employed."[73] Since CSS "actually works" in those instances, it is an "effective" technological measure.[74]

---

[64] 17 U.S.C. §§ 1201(a)(1)(A), (a)(2) (2006).
[65] *Reimerdes*, 111 F. Supp. 2d at 317.
[66] *Id.*
[67] NIMMER, *supra* note 27.
[68] *Reimerdes*, 111 F. Supp. 2d at 318.
[69] *See id.* at 317–18.
[70] *Id.* at 317.
[71] *Id.* at 318.
[72] ANALYSIS OF H.R. 2281, *supra* note 34, at 10.
[73] *See Reimerdes*, 111 F. Supp. 2d at 318.
[74] *Id.*

¶26 Following *Reimerdes*, the entertainment industry giants have used § 1201 to wage a very successful campaign against media pirates. In *321 Studios v. Metro Goldwyn Mayer Studios, Inc.*, several prominent members of the Motion Picture Association of America attained an injunction against the unauthorized distribution of computer software that was capable of both decrypting and copying CSS-protected DVDs.[75] Likewise, Sony successfully invoked § 1201 to obtain an injunction against the owner of a website that sold various devices designed to circumvent the authentication process guarding its PlayStation game consoles.[76]

B. Porous Sieve?

¶27 Based upon the overwhelming success enjoyed by the content owners who have asserted their right to control access under § 1201, one might assume that the statute provides ironclad protection against content thieves. Yet the rather superficial statutory interpretation undertaken by the majority of courts to interpret § 1201 masks a fatal flaw in the statute's language. Upon closer examination, the seemingly foolproof protection of § 1201 appears quite porous.

¶28 In *I.M.S. Inquiry Management Systems, Ltd. v. Berkshire Information Systems, Inc.*,[77] the United States District Court for the Southern District of New York issued a rather shocking ruling. Rather than cut and paste the standard logic employed in the court's *Reimerdes* decision, the panel took a more critical look at the language of the statute.[78] In what may be the first of many losses for the content industry,[79] the court held that

---

[75] 321 Studios v. Metro Goldwyn Mayer Studios, Inc., 307 F. Supp. 2d 1085, 1105 (N.D. Cal. 2004). Plaintiff sought a declaratory judgment that distribution of the software did not violate the DMCA, or, in the alternative, that the anti-circumvention provisions were invalid; plaintiffs were disappointed in both respects. *Id.*

[76] Sony Computer Entm't Am., Inc. v. Divineo, Inc., 457 F. Supp. 2d 957 (N.D. Cal. 2006).

[77] I.M.S. Inquiry Mgmt. Sys., Ltd. v. Berkshire Info. Sys., Inc., 307 F. Supp. 2d 521, 531–33 (S.D.N.Y. 2004).

[78] *See id.* at 532 ("Circumvention requires either descrambling, decrypting, avoiding, bypassing, removing, deactivating or impairing a technological measure qua technological measure. In the instant matter, defendant is not said to have avoided or bypassed the deployed technological measure in the measure's gatekeeping capacity. . . . [Here], what defendant avoided and bypassed was permission to engage and move through the technological measure from the measure's author.").

[79] "*I.M.S.* was correctly decided. Circumvention, as defined in the DMCA, is limited to actions that 'descramble,' 'decrypt,' 'avoid, bypass, remove, deactivate or impair a technological measure.' What is missing from this statutory definition is any reference to 'use' of a technological measure without

the "unauthorized use of an otherwise legitimate, owner-issued password" does not constitute a violation of § 1201.[80] In so doing, it highlighted a potentially devastating chink in the DMCA's armor: § 1201(a)(3).

IV. CHINKS IN THE ARMOR

¶29 The first step in interpreting a statute is to determine whether its language has a plain, unambiguous meaning.[81] "Where the language is plain and admits to no more than one meaning . . . the rules which are to aid in doubtful meanings need no discussion.[82] As Chief Justice Marshall once stated, if the language of the statute is plain, "it *must* be obeyed."[83]

¶30 Section 1201 is unequivocal in its terms. It forbids the circumvention of technological measures that "effectively control" access to copyrighted works[84] and trafficking in certain articles that make such circumvention possible.[85] According to the language of the statute,if the technological measure does not "effectively control[] access to a [copyrighted] work," no amount of circumvention is forbidden.

¶31 Section 1201(a)(3) clearly delineates the bounds of "digital trespass."[86] Both of the access control provisions found in § 1201—the normal anti-circumvention provision found in § 1201(a)(1) and the anti-trafficking provision located in § 1201(a)(2)—are governed by the statutory definitions laid out in § 1201(a)(3). The definitions in § 1201(a)(3) firmly establish the limits of those activities that fall within the purview of the statute's access controls. Section 1201(a)(3) provides:

> (A) to "circumvent a technological measure" means to descramble a scrambled work, to decrypt an encrypted work, or otherwise to avoid, bypass, remove,

---

the authority of the copyright owner, and the court declines to manufacture such language now." Egilman v. Keller & Heckman, LLP, 401 F. Supp. 2d 105, 113 (D.D.C. 2005).

[80] *See I.M.S. v. Berkshire*, 307 F. Supp. 2d at 531–33.

[81] Robinson v. Shell Oil Co., 519 U.S. 337, 340 (1997).

[82] Hamilton v. Rathbone, 175 U.S. 414, 421 (1899).

[83] United States v. Fisher, 6 U.S. (2 Cranch) 358, 386 (1805) (emphasis added).

[84] 17 U.S.C. § 1201(a)(1)(A) (2006) ("No person shall circumvent a technological measure that effectively controls access to a work protected under [Title 17].").

[85] 17 U.S.C. § 1201(a)(2) (2006) ("No person shall manufacture, import, offer to the public, provide or otherwise traffic in any technology, product, service, device, component, or part thereof . . . .").

[86] Chamberlain Group, Inc.v. Skylink Techs., Inc., 381 F.3d 1178, 1196 ("[T]he DMCA created circumvention liability for 'digital trespass' under § 1201(a)(1).").

> deactivate, or impair a technological measure, without the authority of the copyright owner; and
>
> (B) a technological measure "effectively controls access to a work" if the measure, in the ordinary course of its operation, requires the application of information, or a process or a treatment, with the authority of the copyright owner, to gain access to the work.[87]

¶32 The statutory definitions provided in § 1201(a)(3) create two loopholes in the access controls designed to discourage digital piracy. Section 1201(a)(3)(A) provides only a small chink in the DMCA's access-control armor: a relatively narrow definition of "circumvention." Section 1201(a)(3)(B), on the other hand, effectively obliterates whatever protection is left.

A. Circumvention . . . is sometimes possible

¶33 As defined in § 1201(a)(3)(A), circumvention involves any effort 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." Except for descrambling and decrypting, circumvention requires activity outside the normal scope of operation, some action undertaken to avoid the *normal* processes by which the technological measure operates. Mere lack of authority to utilize the process is not enough to trigger § 1201(a)(3)(A).

¶34 One cannot "circumvent a technological measure" simply by utilizing a legitimate password without authorization.[88] Such conduct does *not* avoid or bypass the technological measure; it uses an appropriate key in precisely the manner in which the key was designed to function. The fact that the use of the key was unauthorized is irrelevant because "circumvention" is explicitly limited to the activities listed in § 1201(a)(3)(A).

¶35 The descrambling and decrypting of protected content presents a more difficult problem: *any* unauthorized use of the proper key leads directly to the forbidden activity.[89] The shortcomings of the statutory language with regard to avoidance and bypass are subsumed by the very

---

[87] 17 U.S.C. § 1201(a)(3) (2006).

[88] I.M.S. Inquiry Mgmt. Sys., Ltd. v. Berkshire Info. Sys., Inc., 307 F. Supp. 2d 521, 531–33 (S.D.N.Y 2004). *Contra* Universal City Studios, Inc. v. Reimerdes, 111 F. Supp. 2d 294 (S.D.N.Y. 2000); 321 Studios v. Metro Goldwyn Mayer Studios, Inc., 307 F. Supp. 2d 1085 (N.D. Cal. 2004).

[89] Were it not for § 1201(a)(3)(A)'s explicit inclusion of decryption in the statutory definition, the unauthorized use of even the most complex encryption key might arguably fit into the avoid-bypass loophole.

nature of decryption and descrambling technology. Whereas the use of a key consisting of a simple password allows one to slip through a loophole in the language of the statute, any unauthorized use of a complex encryption key (that succeeds in decrypting the work) amounts to circumvention of a technological measure.[90]

B. Effective Control . . . is virtually nonexistent

¶36 If § 1201(a)(3)(A) was the only statutorily-defined limitation included in the access controls of § 1201, it would be fairly easy for content owners to avoid the "circumvention" loophole and achieve the desired protection. Simply by encrypting or scrambling their data, they could establish a foolproof protection scheme—any unauthorized use of the appropriate decryption/descrambling key would amount to "circumvention," as would any effort to "avoid, bypass, remove, deactivate, or impair" the decryption/scrambling technology. The makers and distributors of decryption/descrambling devices would have virtually no chance of escaping liability.

¶37 Fortunately for all of the scurvy pirates out there, the Information Technology Industry Council lobbied hard for the inclusion of an explicit definition of what constitutes an "effective" technological measure.[91] In particular, they wanted to specify that "effective" technological measures "must be strong, 'active' measures, such as encryption or scrambling, which obscure the content itself."[92] "Implementing legislation that did not draw a clear distinction between 'effective' technological measures and all others," they feared, "would leave us with a Hobbesian choice of producing slow, 'legal' computers or fast, 'illegal' computers."[93] A noble effort for a worthy cause, but it resulted in a second loophole that is *much* bigger than the first!

¶38 Section § 1201(a)(3)(B) states that "a technological measure 'effectively controls access to a work' if the measure, in the ordinary course of its operation, requires the application of information, or a process or a treatment, with the authority of the copyright owner, to gain access to the work."[94] In other words, a technological measure is not "effective" unless

---

[90] This is so because the language of § 1201(a)(3)(A) with regard to descrambling & decrypting is framed in terms of the result achieved, not the action taken.

[91] *See Copyright Treaties Implementation Act: Hearing on H.R. 2281 Before the Subcomm. on Telecomm. Trade, and Consumer Prot. of the H. Comm. on the Judiciary*, 105th Cong.(1998) (statement of Chris Byrne, Silicon Graphics, Inc., on behalf of the Information Technology Industry Council).

[92] *Id.*

[93] *Id.*

[94] 17 U.S.C. § 1201(a)(3)(B) (2006).

it ordinarily requires two things: 1) the application of some information or process, and 2) "the authority of the copyright owner."[95] The inclusion of the latter requirement is effectively a death knell to the anti-circumvention provisions of § 1201.

¶39 Virtually all technological measures require "the application of information, or a process or a treatment."[96] Indeed, it is difficult to imagine the existence of a technological measure that granted access in the absence of such an application. Even the most rudimentary access controls—such as the automatic doors at your local pharmacy—require the application of information (i.e., that you have just broken the plane of its motion detecting radar, or stepped on its pressure-sensitive floor mat) in order to grant access to the user.

¶40 The majority of technological access controls do not, however, require "the authority of the copyright owner." If the appropriate information or process is applied, the technological measure will grant access regardless of whether the party applying the required information or process actually had permission to engage the system. Because the information or process applied to engage the access control is identical in both the legitimate and illicit contexts, the technological measure is not, itself, capable of distinguishing between those two applications. As such, the vast majority of technological measures do not fulfill the latter requirement of § 1201(a)(3)(B), and therefore do *not* "effectively control[] access to a [copyrighted] work."

V. WHAT'S WRONG WITH *REIMERDES?*

¶41 This strict, textual interpretation of § 1201(a)(3) is directly at odds with prior case law, which gave a much broader reading to the language of the statute. In what appears to be an effort to give life to the intent of Congress, the courts interpreting § 1201 have thus far glossed over the critical language of § 1201(a)(3)(B).[97] In *Reimerdes*, for instance, the court completely divorced the technological measure from the authority

---

[95] *Id.*

[96] By definition, a "technological" measure must relate to or involve technology. THE AMERICAN HERITAGE DICTIONARY OF THE ENGLISH LANGUAGE (4th ed. 2004), *available at* http://dictionary.reference.com/browse/technological. Technology, in turn, necessitates the practical application of science or other such information. THE AMERICAN HERITAGE DICTIONARY OF THE ENGLISH LANGUAGE (4th ed. 2004), *available at* http://dictionary.reference.com/browse/technology.

[97] Even the *I.M.S. v. Berkshire* court ignored the authority requirement of § 1201(a)(3)(B). *See* I.M.S. Inquiry Mgmt. Sys., Ltd. v. Berkshire Info. Sys., Inc., 307 F. Supp. 2d 521, 531 (S.D.N.Y 2004).

requirement when it evaluated the "effectiveness" of CSS encryption software:[98]

> One cannot gain access to a CSS-protected work on a DVD without application of the three keys that are required by the software. One cannot lawfully gain access to the keys except by entering into a license with . . . the copyright owners or by purchasing a DVD player or drive containing the keys pursuant to a license. In consequence, . . . CSS 'effectively controls access' to copyrighted DVDs.[99]

This same flawed logic has been rehashed in subsequent cases.[100]

¶42 Section 1201 does *not* contain a separate requirement that the "keys" required to open a technological access control—the information or process required by the technological measure—be "lawfully obtained." Section 1201(a)(3)(B) clearly never addresses how those "keys" were obtained; it requires only that the technological measure actually requires their application. Indeed, the statutory definition of "effective control" is focused solely on the operation of the technological measure itself. There is no mention of content pirates or their ill-gotten "keys."

¶43 The only way to rectify the "effectiveness" analysis of *Reimerdes* with the text of § 1201(a)(3)(B) is to assume that the "ordinary course of [a technological measure's] operation" is limited to situations wherein the party "lawfully gain[s] access to the keys"[101] required to engage that measure. That assumption, however, cannot be valid. Were it true, the validity of that assumption would render the authority requirement of the provision completely superfluous. By explicitly defining "effective" technological measures as those that refuse to grant access in the absence of "the authority of the copyright owner," § 1201 implicitly acknowledges that all technological measures do not contain such a requirement as part of their "ordinary course of operation." Consequently, it is erroneous to assume that the "ordinary course of [CSS] operation" (or that of any other access control) inherently requires permission to engage the technological measure.

¶44 A court must therefore make a factual finding that a given technological measure (*not* the measure's author) in fact requires that the user have authority to use the key as part of its "ordinary course of

---

[98] *See* Universal City Studios, Inc. v. Reimerdes, 111 F. Supp. 2d 294, 317–18 (S.D.N.Y. 2000).
[99] *Id.*
[100] *See, e.g.*, 321 Studios v. Metro Goldwyn Mayer Studios, Inc., 307 F. Supp. 2d 1085, 1095 (N.D. Cal. 2004) (quoting *Reimerdes* for the proposition that CSS is an "effective" technological measure).
[101] *Reimerdes*, 111 F. Supp. 2d at 317–18.

operation." But, as was previously discussed,[102] such a determination must undoubtedly be based upon a legal fiction. In reality, technological measures cannot distinguish between the application of identical information by a legitimate user and a key-thieving pirate.

¶45 It is not enough that the court thinks that the measure *should* require such authority. The statute plainly mandates that the measure must *actually* require "the authority of the copyright owner."

VI. A CALL TO AMEND

¶46 If the DMCA is to provide an effective safeguard for technological access controls, it must be amended to close the loopholes present in § 1201(a)(3). The shortcomings of the statute are not merely semantic—one of the loopholes has already been judicially exposed,[103] and it is only a matter of time before the other is asserted. Indeed, pirates who find themselves accused of violating § 1201—and those generally opposed to the DMCA's access controls—would be wise to mount a defense based upon the technical language of §§ 1201(a)(3)(A) and 1201(a)(3)(B).

¶47 However tempted they may be, courts should resist the urge to judicially rewrite § 1201 to say what they "know" it is supposed to say. "It is emphatically the province and duty of the judicial department to say what the law is,"[104] not what it should be. "Statutory construction must," therefore, "begin with the language employed by Congress and the assumption that the ordinary meaning of that language accurately expresses the legislative purpose."[105] For "where the language of the act is explicit, there is great danger in departing from the words used, to give an effect to the law which may be supposed to have been designed by the legislature."[106]

¶48 Moreover, courts should avoid rushing to judgment about Congress' intentions regarding the access controls (supposedly) embodied in § 1201. Given the current state of unrest amongst content users and legal academics,[107] it would be wise to force Congress to wrestle with the

---

[102] *See supra* pp. 14–15.
[103] *See* I.M.S. Inquiry Mgmt. Sys., Ltd. v. Berkshire Info. Sys., Inc., 307 F. Supp. 2d 521 (S.D.N.Y 2004)..
[104] Marbury v. Madison, 5 U.S. (1 Cranch) 137, 177 (1803).
[105] Park 'n Fly, Inc. v. Dollar Park & Fly, Inc., 469 U.S. 189, 194 (1985).
[106] Denn v. Reid, 35 U.S. 525, 527 (1836).
[107] *See generally* Michael Landau, *Has the Digital Millennium Copyright Act Really Created a New Exclusive Right of Access?: Attempting to Reach a Balance Between Users' and Content Providers' Rights*, 49 J. COPYRIGHT SOC'Y U.S.A. 277 (2001); Jacqueline D. Lipton, *Solving the Digital Piracy*

provisions of § 1201. If Congress truly wishes to provide the U.S. copyright industry with impenetrable access controls, it is certainly free to amend the statute.[108] Simply strengthening the language of § 1201(a)(3) should not be a daunting task—provided, of course, that granting such strong access controls is still the will of Congress.

¶49 The E.U. Directive enacting the relevant portions of the WIPO Copyright Treaty provides one example of language that would aptly express the supposed will of Congress.[109] There, "effective" technological measures are defined as those whereby "the use of a protected work . . . is controlled by the rightholders through application of an access control or protection process . . . which achieves the protection objective."[110] So long as "the protection objective" is defined to be something akin to "a substantial reduction in the likelihood of unauthorized access," adoption of the aforementioned language would extend the protection of § 1201 to virtually all technological access controls.

CONCLUSION

¶50 In its present state, § 1201 does not provide strong legal protection for technological measures designed to prevent the unauthorized access of copyrighted works. With a few minor tweaks in the language of the statute, however, it could become a legitimate bulwark against the ever-increasing threat of digital piracy. The courts, should not be the instrument of that change. Instead, the courts should pursue their traditional duties with increased fervor, faithfully giving life to the plain meaning of § 1201. Leave to Congress the job of closing the loopholes.

Puzzle: Disaggregating Fair Use from the DMCA's Anti-Device Provisions, 19 HARV. J.L. & TECH. 111 (2005).

[108] Indeed, three proposed amendments to the language of § 1201 are already on the floor of Congress. H.R. 1201, 110th Cong. (2007); H.R. 3155, 110th Cong. (2007); S. 2317, 110th Cong. (2007).

[109] *See* Council Directive 2001/29/EC, 2001 O.J. (L 167) 10 (EC).

[110] *Id.* art. 17.