

2-1-2007

# The Pros and Cons of Strengthening Intellectual Property Protection: Technological Protection Measures and Section 1201 of the US Copyright Act

Jane C. Ginsburg  
*Columbia Law school*, [ginsburg@law.columbia.edu](mailto:ginsburg@law.columbia.edu)

Follow this and additional works at: [http://lsr.nellco.org/columbia\\_pllt](http://lsr.nellco.org/columbia_pllt)

 Part of the [Computer Law Commons](#), [Intellectual Property Commons](#), [Public Law and Legal Theory Commons](#), and the [Science and Technology Commons](#)

## Recommended Citation

Ginsburg, Jane C., "The Pros and Cons of Strengthening Intellectual Property Protection: Technological Protection Measures and Section 1201 of the US Copyright Act" (2007). *Columbia Public Law & Legal Theory Working Papers*. Paper 07137.  
[http://lsr.nellco.org/columbia\\_pllt/07137](http://lsr.nellco.org/columbia_pllt/07137)

This Article is brought to you for free and open access by the Columbia Law School at NELLCO Legal Scholarship Repository. It has been accepted for inclusion in Columbia Public Law & Legal Theory Working Papers by an authorized administrator of NELLCO Legal Scholarship Repository. For more information, please contact [tracy.thompson@nellco.org](mailto:tracy.thompson@nellco.org).

[Draft: 20 August 2007]

For Information and Communications Technology Law (UK) (Nov. 2007)

## **The Pros and Cons of Strengthening Intellectual Property Protection: Technological Protection Measures and Section 1201 of the US Copyright Act**

Jane C. Ginsburg\*

### *Abstract*

The announcement in late November 2006 of the Copyright Office's triennial rulemaking to identify "classes of works" exempt from the § 1201(a)(1) prohibition on circumvention of a technological measure controlling access to copyrighted works in part occasions this assessment of the judicial and administrative construction of this chapter of the 1998 Digital Millennium Copyright Act. The current Rulemaking appears more innovative than its predecessors, particularly in defining the exempted "class of works" by reference to the characteristics of the works' users. Copyright owner overreaching or misuse may also underlie the relative vigor of this Rulemaking: if producers of devices or providers of services seek to leverage into *de facto* monopolies over utilitarian articles the protection of access controls on computer programs that in turn control the function of these objects, then the courts and the Librarian of Congress through the Copyright Office will need to exercise countervailing vigilance in interpreting the statute. Fortunately, Section 1201 is not so hermetically drafted as to resist all attempts to introduce flexibility; this article suggests some approaches to offset overly literalist statutory construction. Notably, the emergence of fair use as a limiting norm of extra-copyright application, as evidenced in the Trademark Dilution Revision Act of 2006, suggests that judges may yet devise ways of reconciling broader intellectual property rights with principles of free expression. Those who interpret the statute should nonetheless bear in mind the many new business models that Congress foresaw and that digital rights management measures (some of them author-empowering) have in fact enabled, lest insecurity dampen the prospects for these models' development.

### I. Introduction

The 1998 "Digital Millennium Copyright Act" brought a variety of modifications to the US copyright law. Despite the DMCA's general reputation as a copyright-reinforcing law, many of those modifications in fact aimed to immunize certain industries from infringement claims,<sup>1</sup> or to adapt extant compulsory licenses to evolving digital communications.<sup>2</sup> The principal copyright-strengthening portion of the DMCA is found

---

\* Morton L. Janklow Professor of Literary and Artistic Property Law, Columbia University School of Law. This article was initially prepared for a symposium on "The Pros and Cons of Strengthening Intellectual Property Protection," held at Waseda University, Dec. 15, 2006, and is in part adapted from *Legal Protection of Technological Measures Protecting Works of Authorship: International Obligations and the US Experience*, 29 Columbia J. L. & Arts 11 (2005). Thanks for research assistance to Kevin Burdette and Keith Bradley, both Columbia Law School class of 2007, and to Jeff Vernon, Columbia Law School class of 2008.

<sup>1</sup> See the Online Service Provider Liability Limitation Act, 17 USC § 512.

<sup>2</sup> See 17 USC §§ 114, 115 provisions on digital phonorecord deliveries.

in chapter 12 of the copyright act, creating a new regime of protection for technological measures that protect copyrighted works. Chapter 12 has attracted considerable attention – much of it hostile -- from commentators and even the popular press.<sup>3</sup> But it may also have provided the legal environment for new business models to flourish. The best-known and spectacularly successful example of these is the iTunes music delivery service. The following discussion will examine the Section 1201 regime. After a quick review of what the law provides, I will examine how it has been working in practice, through its judicial and administrative interpretation. Section 1201 presents an excellent case study of the benefits and dangers of strengthening copyright protection.

## II. Protected Subject Matter and Prohibited Acts

**Statutory text:** Section 1201 defines three new violations:<sup>4</sup> (a)(1) to circumvent

---

<sup>3</sup> See, e.g., Lawrence Lessig, *Jail Time in the Digital Age*, N.Y. Times, July 30, 2001, at A17; see also Anick Jesdanun, *Copyright act draws complaints: Digital-use law called too broad*, Seattle Times, December 21, 2001, at C6; Dan Gillmor, *Hacking, Hijacking our Rights*, San Jose Mercury News, July 28, 2002, at 1F.

4. Section 1201 provides, in relevant part:

*§ 1201. Circumvention of copyright protection systems*

*(a) Violations Regarding Circumvention of Technological Measures.*

(1)(A) No person shall circumvent a technological measure that effectively controls access to a work protected under this title. The prohibition contained in the preceding sentence shall take effect at the end of the 2-year period beginning on the date of the enactment of this chapter. . . .

(2) 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 this title;

(B) has only limited commercially significant purpose or use other than to circumvent a technological measure that effectively controls access to a work protected under this title; or

(C) is marketed by that person or another acting in concert with that person with that person's knowledge for use in circumventing a technological measure that effectively controls access to a work protected under this title.

(3) As used in this subsection—

(A) 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; 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.

*(b) Additional Violations.* (1) 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 protection afforded by a technological measure that effectively protects a right of a copyright owner under this title in a work or a portion thereof;

(B) has only limited commercially significant purpose or use other than to circumvent protection afforded by a technological measure that effectively protects a right of a copyright owner under this title in a work or a portion thereof; or

(C) is marketed by that person or another acting in concert with that person with that person's knowledge for use in circumventing protection afforded by a technological measure that effectively protects a right of a copyright owner under this title in a work or a portion thereof.

(2) As used in this subsection—

(A) to “circumvent protection afforded by a technological measure” means avoiding, bypassing, removing, deactivating, or otherwise impairing a technological measure; and

(B) a technological measure “effectively protects a right of a copyright owner under this title” if the

technological protection measures that control access to copyrighted works; (a)(2) to manufacture, disseminate or offer, etc., devices or services, etc., that circumvent access controls and (b) to manufacture, disseminate, or offer, etc., devices or services, etc., that circumvent a technological measure that “effectively protects a right of the copyright owner . . . .” It is important to appreciate that these violations are distinct from copyright infringement. The violation occurs with the prohibited acts; it is not necessary to prove that the dissemination of circumvention devices resulted in specific infringements or that the purpose of circumventing an access control was to commit an infringing act. On the other hand, section 1201 also sets out a long, disparate (and somewhat incoherent) list of exceptions to the prohibition on circumvention of access controls.<sup>5</sup> Section 1201 thus appears to expand the scope of copyright in the following ways:

1. It creates a claim for unauthorized access to works of authorship;
2. It makes distributors of circumvention devices directly liable for the dissemination of the means to gain unauthorized access;
3. It makes distributors of circumvention devices directly liable for the dissemination of the means to make copies or to engage in communications to the public;
4. It makes disseminators of both kinds of devices liable even if some of the end users to whom the devices are distributed would employ the devices for non-infringing purposes.

To appreciate the actual scope of section 1201, it is necessary to inquire further into the subject matter of its protection, into the acts it prohibits and into its accommodation of copyright exceptions. That inquiry will allow us better to assess whether section 1201, at least as experienced so far, has over-expanded the reach of copyright or, rather, has enabled copyright to adapt to the challenges and opportunities that digital media present.

**Subject matter protected:** We have seen that section 1201 covers two different kinds of protective measures, those that “effectively control access to a work protected under this title [the Copyright Act],” and those that “effectively protect a right of a copyright owner,” i.e., that protect against copying and communicating to the public. Judicial decisions construing section 1201 have considered what it means to protect “effectively.” They also have addressed whether the object of the access control measure is a “work protected under this title.”

**“Effectively protect:”** With respect to effective protection, the courts are unanimous that

---

measure, in the ordinary course of its operation, prevents, restricts, or otherwise limits the exercise of a right of a copyright owner under this title.

17 U.S.C. § 1201 (1998). For a discussion of the legislative history of Section 1201, and of proposals that preceded it, see June Besek, *Anti-Circumvention Laws and Copyright: A Report From the Kernochan Center for Law, Media and the Arts*, 27 Colum. J.L. & Arts 389, 400-07 (2004) [hereinafter, Besek, *Anti-Circumvention Laws*].

5. 17 USC § 1201(d)-(j) (1998).

“effective” protection does not mean protection that is especially difficult to crack.<sup>6</sup> In *Lexmark v. Static Controls Corp.*, a decision concerning the circumvention of a code controlling access to the functions of a printer, however, the Sixth Circuit Court of Appeals observed that because the printer engine program was accessible by other means, the lock-out code could not be deemed “effective.”<sup>7</sup>

**Controlling access to a work of authorship:** The *Lexmark* case is most significant for its analysis of the second issue—whether the technological measure controls access to a work protected under the Copyright Act. In notorious but, happily, unsuccessful attempts to leverage the DMCA into protecting the “aftermarket” for spare and replacement parts, the producers of printers and cartridges, in one case, and of garage door openers, in the other,<sup>8</sup> asserted that rival printer cartridge and door opener manufacturers had violated the DMCA’s prohibition on circumvention of access controls. In both cases, the spare part in question would not interact with the host device unless the host device recognized the spare part as authorized to function together with the host device. If the spare part entered the appropriate authentication sequence or, in the terms of a frequently-used metaphor, engaged in the “secret handshake” with the host device, then the host would be “fooled” into “thinking” that it was working with a component made by the same producer and would allow the component to perform its intended function. The “secret handshake” thus made it possible for a rival printer cartridge to substitute for the printer producer’s own replacement cartridges, and for a “universal garage door opener” to open the remote controlled garage doors installed by a rival company.

Now, what have printer cartridges and garage doors to do with copyright? Nothing, except, emphasized the plaintiffs, that computer programs control the functioning of these devices, and computer programs are copyrighted works. The extraordinary consequence of plaintiffs’ reasoning is that any useful object whose workings are controlled by computer programs—and today, that means an endless variety of consumer and industrial goods—can come within the scope of section 1201 if the object’s producer makes access to those programs subject to an authentication sequence. As a policy matter, this result is inconceivable. Among other things, Congress has persistently

---

6. 321 Studios v. MGM, 307 F.Supp. 2d 1085, 1095 (N.D. Cal. 2004); Universal Studios v. Reimerdes, 111 F.Supp. 2d 346, 317-18 (S.D.N.Y. 2000), *aff’d sub nom.*, Universal City Studios, Inc. v. Corley, 273 F.3d 429 (2d Cir. 2001) (rejecting as “spurious” the claim that DVD protection code did not “effectively” protect DVDs because a Norwegian teenager easily cracked it); Sony Computer Entertainment v. Divineo, -- F.Supp. 2d --, 2006 WL 2987672 (ND Cal. Sept. 11, 2006)(rejecting contention that wide availability of circumvention devices makes a technological protection measure “ineffective”).

7. *Lexmark Int’l. v. Static Control Components, Inc.*, 387 F.3d 522 at 547 (6th Cir. 2004). The court also stated “one would not say that a lock on any door of a house ‘controls access’ to the house after its purchaser receives the key to the lock.” *Id.* This proposition is questionable: the lock continues to control access to those who do not have keys. On remand from the Fed. Cir., the District Court in *Storage Technology v Custom Hardware*, -- F.Supp.2d -- (D. Mass. 2006) followed the 6<sup>th</sup> Circuit in ruling that when access to the copyrighted work (in this instance, computer code) is otherwise available (in this instance on floppy disks), a measure controlling access by some other means is not “effective.”

8. *Chamberlain Group v. Skylink Techs.*, 381 F.3d 1178 (Fed. Cir. 2004).

Professor Randal Picker has pointed out the kinship between the *Lexmark* and *Chamberlain* DMCA cases and previous (unsuccessful) attempts to convert controversies about competition in the spare and replacement parts markets into copyright infringement claims. See Randal C. Picker, Copyright and the DMCA: Market Locks and Technological Contracts, available at [http://papers.ssrn.com/sol3/papers.cfm?abstract\\_id=690901&high=%20picker](http://papers.ssrn.com/sol3/papers.cfm?abstract_id=690901&high=%20picker) (discussing, *inter alia*, *Toro Co. v. R&R Prods. Co.*, 787 F.2d 1208 (8<sup>th</sup> Cir 1986) and *Southco Inc. v. Kanebridge Corp.*, 390 F.3d 276 (3d Cir 2004)).

declined to legislate design protection, in part because of its inability to resolve the spare parts issue;<sup>9</sup> Congress is unlikely to have sought the result of an exceptionally strong design protection regime through the stealthy means of the DMCA.

But does the *text* of section 1201 permit this result? The computer program that controls the functioning of the consumer product may indeed be a copyrighted work. The *Lexmark* court held that the authentication sequence was insufficiently original to be protectable but that the printer program was copyrightable. Nonetheless, that was not sufficient to bring the access control within the scope of section 1201. In a common sense interpretation of the text, the court reviewed earlier “secret handshake” cases, involving access to transmissions of recordings of musical works, to videogames and to motion pictures on DVDs. The court underscored that all of those cases involved circumvention of access to computer programs that were “conduit[s] to protectable expression.”<sup>10</sup> In the printer cartridge case, by contrast, invocation of the computer program was clearly pretextual: operating the program did not make it possible to see, hear or otherwise engage with a work of authorship. Rather, “the program’s output is purely functional: [it] ‘controls a number of operations’ in the Lexmark printer.”<sup>11</sup>

**Nature of the access that the measure controls:** The court in the garage door opener case reached the same result, but for different reasons. Where the *Lexmark* court focused on the “work” that is the object of the access control, the court in *Chamberlain v Skylink* addressed the *purpose* of the access that the technological measure controls. The court interpolated into section 1201 a requirement that the protection against circumvention of an access control be related to protection against infringement. To the extent that access controls forestall infringement, for example, by making unauthorized copies unplayable and therefore futile, the access control comes within the scope of section 1201. But if the uses that the access control cuts off are not infringing uses, then the access control is not one that section 1201 was designed to protect, the court determined.<sup>12</sup> In the case of garage door openers, this distinction makes some sense: using the opener does not infringe any copyrights. But, as applied to access controls that are “conduits” to works of authorship, the proposition is in some tension with Congress’s goals in prohibiting the circumvention of those technological measures. The *Chamberlain* court worried that interpreting section 1201 to create an independent violation for circumventing access controls (or disseminating access circumvention devices) would “effectively create two distinct copyright regimes,” one tied to the traditional rights of copyright owners (section 1201(b)), and the other allowing copyright owners “unlimited rights to hold circumventors liable under § 1201(a) merely for accessing that work, even if that access enabled only rights that the Copyright Act grants to the public.”<sup>13</sup>

---

9. See 17 U.S.C. § 1301-1302 (2000), for the closest Congress has come, setting out a *sui generis* regime limited to the protection of boat hull designed.

10. *Lexmark*, 387 F.3d at 547-48.

11. *Id.* at 548.

12. *Chamberlain*, 381 F.3d at 1197-1201. The Federal Circuit reiterated this analysis in *Storage Technology Corp. v. Custom Hardware Engineering & Consulting, Inc.*, 421 F.3d 1307 (Fed. Cir. 2005) (circumvention of code controlling access to data library maintenance software held not to violate § 1201 because access does not “facilitate copyright infringement”: copies made in RAM once software is accessed are copies permitted under the § 117(c) exception for computer maintenance).

13. *Chamberlain*, 381 F.3d at 1200-01.

But there is considerable evidence from the text and from the legislative history that Congress did intend to create an additional copyright regime based on the control over access to digitally distributed works of authorship. The text indicates that the “access” that section 1201(a) protects goes beyond traditional copyright prerogatives; it distinguishes “access” from a “right of the copyright owner under this title.” Some activities subject to access controls do not implicate traditional copyright owner rights such as reproduction and public performance. For example, an access control may limit the number of viewings of a motion picture distributed on a DVD. But if the viewings occur at home, they likely do not come within the traditional scope of exclusive rights. Thus, suppose I purchase a time-loaded or limited-viewing DVD, for a lower price than an unlimited viewing DVD, and that I circumvent an access protection in order to obtain an unlimited number of private viewings of the film for an unlimited time. I have not committed copyright infringement, because the public performance right does not reach the extra viewings. I have, however, defeated the purpose of offering the film on a pay-per-view or similar basis. The legislative history indicates that the DMCA was designed in part specifically to foster a variety of business models offering the public a diversity of levels of access, for a diversity of prices. As the House Commerce Committee reported:

[A]n increasing number of intellectual property works are being distributed using a “client-server” model, where the work is effectively “borrowed” by the user (e.g., infrequent users of expensive software purchase a certain number of uses, or viewers watch a movie on a pay-per-view basis). To operate in this new environment, content providers will need both the technology to make new uses possible and the legal framework to ensure they can protect their work from piracy.<sup>14</sup>

“In other words,” my Columbia University colleague June Besek has explained, “providing copyright owners with the ability to preclude unlimited access was a goal of the DMCA, not just an unforeseen and unfortunate consequence.”<sup>15</sup> This appears to be true, even when some of the precluded access would not result in copyright infringement. On the other hand, it does not necessarily follow that Congress intended to grant copyright owners general rights to control all digital “uses” of protected works. But to the extent that access is a precondition to “use” or enjoyment of a work, protecting against circumvention for some non infringing purposes (such as private listening, viewing, or playing a work) may effectively grant copyright owners extremely broad extra-copyright rights compromising all non infringing uses. Finding the balance between encouraging and securing new markets for digital works on the one hand, and empowering copyright owner overreaching on the other, will be a difficult task for courts and, as we shall see, for the Copyright Office. The farther away the access-protected work from the type of creative works that form the core of copyright, moreover, the more likely that protecting the code that conditions access to the work will lead to results not only unattainable under but also incompatible with traditional copyright law. The most current example of this tension, which we shall explore in greater detail later, is the technological measures embedded in cell phones that condition access to computer programs which in turn control access to wireless networks.

---

14. H.R. REP. NO. 105-551, pt. 2, at 23 (1998).

15. Besek, *Anti-Circumvention Laws*, *supra* note 4, at 474.

**Acts prohibited:** Section 1201 prohibits the *act* of circumventing an access control and the “*trafficking*” in devices that circumvent either access controls or “rights” controls. It does not prohibit the act of circumventing a rights control, in part because the results of that act will be directly infringing (or will qualify for an exception), and in part because the most economically significant act is the distribution of the device that will allow the end-user to circumvent. By contrast, circumvention of an access control does not directly result in an infringement. If circumvention of an access control is not unlawful, then, arguably, dissemination of a device that enables circumvention of an access control would not be wrongful either. By making the act of access circumvention unlawful, the DMCA lay a stronger foundation for prohibiting the dissemination of enabling devices as well.

**Circumvention:** While most of the cases involve circumvention devices, a few cases have arisen concerning the act of circumvention.<sup>16</sup> Although some courts have held that an unauthorized person’s use of an actual password does not “circumvent,”<sup>17</sup> this interpretation appears inconsistent with the statute. Section 1201(a)(3)(A) defines “to circumvent” as “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*” (emphasis supplied). Entry of the password “deactivates” the measure that restricts access;<sup>18</sup> if the password is employed by an unauthorized user, then the deactivation will not have occurred with the copyright owner’s authority.<sup>19</sup>

**Devices:** Section 1201(a)(2) and (b) do not prohibit the dissemination of every device that *might* be used to defeat an access or rights control. These provisions do not target general purpose devices whose accidental, incidental or unwitting use results in circumvention. Nor does it bar those devices that, while capable of, and even used for, circumvention, are primarily designed or used for other purposes. The law prohibits the manufacture and trafficking in devices and services in the following three circumstances:

1. The device was “primarily designed or produced for the purpose of circumventing a technological measure that effectively controls access” to a copyrighted work or “effectively protects a right of the copyright owner”; or

---

16. In one case, the plaintiff brought an action seeking a declaratory judgment that the section 1201(a)(1) was unconstitutional because it restrained his First Amendment right to reverse engineer software that blocked access to certain Internet sites in order to publish a list of the blocked sites. The court held the complaint too vague to give rise to an adjudicable “case or controversy.” *Edelman v. N2H2*, 263 F.Supp. 2d 137 (D.Mass. 2003). In any event, it is likely plaintiff’s conduct would have benefited from statutory and administrative exceptions to sec. 1201(a). See Besek, *Anti-Circumvention Laws*, *supra* note 4, at 414-15.

17. *IMS Inquiry Mgmt. Sys. v. Berkshire Info. Mgmt. Sys.*, 307 F.Supp. 2d 521 (SDNY 2003). Accord, *Egilman v. Keller & Heckman*, 401 F.Supp.2d 105 (DDC 2005).

18. A password-controlled access measure fits the statutory definition of a technological measure that effectively controls access to a work. See 17 U.S.C. § 1201(a)(3)(B).

19. See, e.g., *321 Studios v. MGM*, 307 F.Supp. 2d 1085, 1098 (N.D. Cal. 2004) (“321 states that its software does not avoid, bypass, remove, deactivate, or otherwise impair a technological measure, but that it simply uses the authorized key to unlock the encryption. However, while 321’s software does use the authorized key to access the DVD, it does not have authority to use this key, as licensed DVD players do, and it therefore avoids and bypasses [the] CSS [access control].”).

2. The device, albeit not *primarily* designed to circumvent, in fact “has only limited commercially significant purpose or use other than to circumvent . . .”; or

3. The device is “marketed” (i.e., advertised or promoted) as a device to be used to circumvent access or rights controls. In this case, the target of the law is the person promoting the circumventing use; it is not the manufacturer or distributor of the device, unless that person acts in concert with the marketer.

Many of the cases that have arisen have involved rather obvious circumvention devices, such as cable and satellite descramblers<sup>20</sup> and devices designed to neutralize the access controls on DVDs.<sup>21</sup> As a result, they have not required courts to determine whether the primary purpose or actual use of the device was to circumvent.<sup>22</sup> Courts have interpreted the text of section 1201 to reach trafficking in circumvention devices regardless of whether the circumventions that the devices enable would result in infringements. Thus, for example, in one of the DVD cases, *321 Studios v. MGM*, the court stated the following:

a simple reading of the statute makes it clear that its prohibition applies to the manufacturing, trafficking in and making of devices that would circumvent encryption technology, not to the users of such technology. It is the technology itself at issue, not the uses to which the copyrighted material may be put. This Court finds . . . that legal downstream use of the copyrighted material by customers is not a defense to the software manufacturer’s violation of the provisions of § 1201(b)(1).<sup>23</sup>

Similarly, in *Sony Computer Entertainment v. Divineo*, the court deemed irrelevant defendant’s invocation of potential non infringing use of its “mod chips” to override region coding or to ensure that the Sony PlayStation would interoperate with independent computer programs.<sup>24</sup> (One suspects, however, that the principal use of the “mod chips” was to allow the Playstation to play unauthorized copies of PlayStation games, just as the likely use of the 321 Studio device was not to make “backups” of purchased copies, but to allow the DVD player to run unauthorized copies.<sup>25</sup>)

---

20. See, e.g., *Coxcom v. Chaffee*, 2006 WL 1793184 (D.R.I.); *DirecTV v. Borrow*, 2005 U.S. Dist. LEXIS 1328 (N.D. Ill. 2005); *Comcast of Ill. v. Hightech Electronics*, 2004 U.S. Dist. LEXIS 14619 (N.D. Ill. 2004); *DirectTV v. Ferguson*, 328 F.Supp. 2d 904 (N.D. Ind. 2004).

21. See, e.g., *Universal Studios v. Corley*, 273 F.3d 429 (2d Cir. 2001); *321 Studios v. MGM*, 307 F.Supp. 2d 1085 (N.D. Cal. 2004); *Macrovision v. Sima*, -- F.Supp.2d -- (SDNY 2006). See also *Automotive Inspection Services, Inc. v. Flint Auto Auction, Inc.*, 2006 U.S. Dist. LEXIS 83056 (E.D. Mich. 11/15/06) (granting a TRO under § 1201(a) because the defendant apparently hacked the plaintiff’s auto inspection software to use it beyond the term of the license).

22. See *DirecTV v. Little*, 2004 U.S. Dist. LEXIS 16350 (N.D. Cal. 2004), for an exception in which the court determined that there was a factual dispute concerning whether the defendant’s “smart cards” were “primarily designed for signal theft.”

23. 307 F.Supp. 2d at 1097-98 (citing *Corley*, 273 F.3d at 443; *U.S. v. Elcom*, 203 F.Supp. 2d 1111, 1120 (N.D. Cal. 2002)).

<sup>24</sup> *Supra*, note 6 at \*7. See also *Macrovision* (defendant’s “CopyThis” and “GoDVD” devices that strip macrovision protection from DVDs held to violate § 1201(b); “Sima’s defense that it only intends to enable ‘fair use’ copying of copyrighted works is no defense at all . . .”).

<sup>25</sup> Similarly, in *Macrovision*, defendant’s assertion that the device enabled back up copying seemed pretextual.

In most of the cases, moreover, the relationship between the circumvention that the device enabled and infringement was fairly apparent. For example, in one of the first cases decided under sec. 1201, *RealNetworks v. Streambox*,<sup>26</sup> the defendant's device imitated the "secret handshake" giving access to recorded music transmitted from the RealNetworks server. Unlike a Real Player, through which a customer could listen to the transmissions, but not copy them, the defendant's system ignored the Real server's "copy switch," enabling its customers to make unauthorized copies of the recorded music. In *321 Studios v. MGM*, the access circumvention device allegedly allowed users to make playable "backup copies" of DVDs that they had purchased, but there is no general copyright exception permitting the creation of "backup copies."<sup>27</sup> Moreover, protestations that the device simply facilitated lawful uses lost credibility in light of 321's "spam" promotion of the device under the slogan, "Never buy another DVD again!"<sup>28</sup>

A more debatable condemnation of an access-circumvention device occurred in another early case, *Sony Computer Ent. v. Gamemasters*.<sup>29</sup> Defendants sold a "Game Enhancer" device that allowed users to alter the real-time play of a videogame (without preserving the modifications) and that also allowed users to override Sony's "region coding," so that a game purchased in a differently-coded region, such as Europe or Japan, could nonetheless be played on a US PlayStation console. Sony claimed that the device that overrode the region-coding also made it possible to play counterfeit copies of PlayStation games, but little evidence supported this contention. The court granted a preliminary injunction on the ground that defendant's device neutralized an access control; the court did not inquire into whether a game lawfully acquired in one region could be played in another without infringing copyright. Both the "first sale" (or "exhaustion") doctrine,<sup>30</sup> and the confinement of the performance right to *public* performances, however, suggest that the copyright owner's exclusive rights do not extend to determining the geographical zones in which members of the public may privately view lawfully made copies. Applying section 1201(a) to protect against circumvention of access measures that limit those copies to playback devices licensed for a given territory thus results in a scope of protection not otherwise available under the copyright act.

But if region-coding is obnoxious, cannot much the same objection be made regarding access measures that control pay-per-view and similar schemes based on price discrimination? The answer may turn on the existence of evidence that Congress sought to protect the latter business models,<sup>31</sup> while similar evidence does not appear to exist regarding the former. Moreover, the latter business models are built on a *quid pro quo*: the extent of access allowed turns on the price the consumer pays. Price discrimination does not appear to characterize region-coding; the consumer is not offered world-wide access at one price, and geographically restricted access at a different, lower, price.

---

26. *RealNetworks v. Streambox*, 2000 U.S. Dist. LEXIS 1889 (W.D. Wash. Jan. 18, 2000).

27. 17 U.S.C. § 117 (2000) permits archival copying of computer programs, but not every work expressed in 1s and 0s is a "computer program." See *Elcom*, 203 F.Supp. 2d at 1135.

28. email forwarded from student, with inquiry "Can they do this?"

29. 87 F.Supp. 2d 976 (N.D. Cal. 1999).

30. See 17 U.S.C. § 109(a) (2000).

31. See Jane C. Ginsburg, Copyright and Control Over New Technologies of Dissemination, 101 COLUM. L. REV. 1613, 1633 n.83 (2001).

These responses do not, however, contradict the basic observation that, by protecting against the circumvention of access controls, without further requiring proof of a nexus between the circumvention and infringement, Congress has permitted, indeed encouraged, copyright owners to create and control markets for their works that the traditional exclusive rights under copyright would not secure. Whether this is a good thing or a bad thing may depend on whether, overall, more works become available to more consumers, under a greater variety of terms, conditions and prices, than were available without legally protected technological protection measures.<sup>32</sup>

### III. Exceptions to Anti Circumvention Protections

Even so, there is another trade-off to consider. Is this flourishing of new owner-controlled copyright markets compatible with the various exceptions that limit the reach of copyright law in a variety of circumstances? Do we get more works for less money, but less freedom to quote from, teach from, build on, study, criticize and even ridicule them? To assess the impact on copyright exceptions of legal protection for technological protection measures, we have first to distinguish section 1201's treatment of circumvention of rights controls from that of access controls. With respect to access controls, section 1201(a) reaches both the end-users who directly circumvent those controls and the persons who manufacture, distribute and market devices primarily designed or used to circumvent those controls. On the other hand, section 1201(d)-(j) includes several exceptions to these prohibitions. Do these exceptions, as construed by the courts, adequately accommodate desirable, albeit unauthorized, uses of copyrighted works?

With respect to rights controls, section 1201(b) does not reach end-users who either directly circumvent rights controls or employ devices to effect that circumvention. Thus, an end-user who circumvents a copy control and then makes a copy or communication that is permissible under the fair use doctrine or other applicable exception is liable neither for a circumvention violation nor for copyright infringement. An end-user who circumvents a copy control to make an unexcused copy or communication to the public will not be liable for a circumvention violation, but will be liable for copyright infringement. On the other hand, the prohibition on trafficking in rights control circumvention devices may make it difficult for many end-users to obtain and utilize the devices regardless of the purpose to which they would put them. Does the prohibition on distribution of devices primarily designed or used to circumvent rights controls therefore stifle copyright exceptions and the beneficial uses those exceptions foster?

**Exceptions to circumvention of access controls:** The DMCA provides a variety of exceptions, including for reverse engineering, encryption research and security testing.<sup>33</sup>

---

32. For a general critique of arguments that price discrimination can justify the creation or reinforcement of intellectual property rights, see Wendy J. Gordon, *Intellectual Property as Price Discrimination: Implications for Contract*, 73 CHI-KENT L. REV. 1367 (1998).

33. See, e.g., Jane C. Ginsburg, *Copyright Legislation for the "Digital Millennium,"* 23 COLUM. J.L. & ARTS 137, 148-52 (1999), for a fuller description of these, and the other, exceptions to 17 U.S.C. § 1201(a) (2000).

The § 1201(f) exception for reverse engineering<sup>34</sup> permits the circumvention of access controls for the sole purpose of creating non-infringing interoperable programs. This provision appears to offer a significant safety valve, notably because it also permits both development of devices necessary to effect the permitted reverse engineering, and distribution of the fruits of the permitted reverse engineering.<sup>35</sup> Nonetheless, the case law construing § 1201(f) remains fairly sparse. In *Davidson & Assoc. v. Internet Gateway*<sup>36</sup> the defendants, having gained access by reverse engineering the plaintiff's control program, did not qualify for the exception because they made infringing copies of the plaintiff's work. Defendants broke the access code of the Battle.net online videogame service in order to develop a Battle.net "emulation site" that would allow owners of copies of the Blizzard videogame to play their games online, without the advertisements and use restrictions imposed by the Battle.net site. Battle.net required users to enter an authentication sequence that would permit the website to verify that the user's copy of the game was authorized. Thus, Battle.net screened out unauthorized copies and did not allow them access to the game site. Defendants' "bnetd" alternative site did not require users to enter the authentication sequence; as a result, owners of "counterfeit" as well as legitimate copies could join in a multiplayer game environment that replicated the desirable aspects of the Battle.net experience. The district court held that the output of the "bnetd" program infringed that of the Battle.net program because there were "no differences between Battle.net and the bnetd emulator from the standpoint of a user who is actually playing the game."<sup>37</sup> The Eighth Circuit affirmed the finding of infringement, albeit without additional analysis.

---

34. 17 U.S.C. § 1201(f) provides:

(f) Reverse Engineering.

- (1) Notwithstanding the provisions of subsection (a)(1)(A), a person who has lawfully obtained the right to use a copy of a computer program may circumvent a technological measure that effectively controls access to a particular portion of that program for the sole purpose of identifying and analyzing those elements of the program that are necessary to achieve interoperability of an independently created computer program with other programs, and that have not previously been readily available to the person engaging in the circumvention, to the extent any such acts of identification and analysis do not constitute infringement under this title.
- (2) Notwithstanding the provisions of subsections (a)(2) and (b), a person may develop and employ technological means to circumvent a technological measure, or to circumvent protection afforded by a technological measure, in order to enable the identification and analysis under paragraph (1), or for the purpose of enabling interoperability of an independently created computer program with other programs, if such means are necessary to achieve such interoperability, to the extent that doing so does not constitute infringement under this title.
- (3) The information acquired through the acts permitted under paragraph (1), and the means permitted under paragraph (2), may be made available to others if the person referred to in paragraph (1) or (2), as the case may be, 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 under this title or violate applicable law other than this section.
- (4) For purposes of this subsection, the term "interoperability" means the ability of computer programs to exchange information, and of such programs mutually to use the information which has been exchanged.

<sup>35</sup> See § 1201(f)(2)(3).

<sup>36</sup>. 334 F.Supp. 2d 1164 (E.D. Mo. 2004), *aff'd.*, 422 F.3d 630 (8th Cir. 2005).

<sup>37</sup>. 334 F. Supp. 2d at 1185.

It is not entirely clear that the defendant's use in that case in fact exceeded the scope of the reverse engineering exception. Assuming he had lawfully obtained a copy of the Blizzard and/or Battlenet programs, the defendant appears to have accessed the program's code "for the sole purpose of identifying and analyzing those elements of the (Battle.net) program that are necessary to achieve interoperability of an independently created computer program (bnetd) with other programs (its users' copies of Blizzard)."<sup>38</sup> Defendant was entitled to do this "to the extent any such acts of identification and analysis do not constitute infringement under this title."<sup>39</sup> The decision does not demonstrate that the defendant's *analysis* was infringing; rather, the *results* of the analysis may have produced a program too similar to the plaintiff's. On the other hand, the exception would not make very much sense if it did not take into account whether the program that results from accessing and studying the plaintiff's code is infringing. The case law developing a fair use exception for reverse engineering, for example, assesses whether the result of the reverse engineering is an independent, non-infringing program (similar in functionality but not expression).<sup>40</sup> Moreover, the court's decision is generally consistent with the rationale for protecting access controls in the first place: to render unauthorized copies useless because the access control will not permit the copies to be viewed or otherwise enjoyed. In this case, the Battle.net authentication sequence rendered unauthorized copies of Blizzard relatively useless because they would not be admitted to the online multiplayer site. Defendant's bnetd site allowed those copies to be played, thus defeating the purpose of the access control.

**Copyright Office rulemaking:** While the exceptions to section 1201(a) are multiple, they are also very narrowly defined and do not invite expansive judicial construction.<sup>41</sup> As a result, Congress instructed the Librarian of Congress, in consultation with the Register of Copyrights, to conduct a rulemaking every three years, both to identify particular "classes of works" whose users would be "adversely affected by the prohibition . . . in their ability to make non infringing uses under this title," and to suspend the application of the prohibition on the act of access control circumvention as to those works until the next rulemaking period.<sup>42</sup> The burden of proving the need for the exemption falls on the proponent.<sup>43</sup> Each rulemaking is *de novo*: a class identified in a prior rulemaking is not automatically reinstated; the Copyright Office must determine whether a need for an exemption continues to be demonstrated. It is important to recognize, however, that the prohibitions against trafficking in access circumvention devices continue to apply.

The most recent rulemaking, issued by the Librarian of Congress on November 20, 2006, gives important additional definition to the term "class of works":

---

38. *Id.* at 1184.

39. *Id.*

40. *See, e.g.,* Sega Enters. Ltd. v. Accolade, Inc., 977 F.2d 1510 (9th Cir. 1992); Sony Computer Entm't, Inc. v. Connectix Corp., 203 F.3d 596 (9th Cir. 2000).

41. *See* 17 U.S.C. § 1201(a)(1)(B)-(E) (2000). *But see* TAN 57-74, *infra* (suggesting possibility of judicial articulation of "fair circumvention" exception).

42. 17 U.S.C. § 1201(a)(1)(C) (2000). For a fuller discussion, *see* Besek, *Anti-Circumvention Laws*, *supra* note 4, at 416-23.

<sup>43</sup> *See* Library of Congress, Copyright Office, 37 CFR Part 201, [Docket No. RM 2005-11], Exemption to Prohibition on Circumvention of Copyright Protection Systems for Access Control Technologies at 5 [hereafter 2006 Rulemaking], [http://www.copyright.gov/1201/docs/fedreg\\_notice.pdf](http://www.copyright.gov/1201/docs/fedreg_notice.pdf)

In the current proceeding, the Register has concluded that in certain circumstances, it will also be permissible to refine the description of a class of works by reference to the type of user who may take advantage of the exemption or by reference to the type of use of the work that may be made pursuant to the exemption. The Register reached this conclusion in reviewing a request to exempt a class of works consisting of “audiovisual works included in the educational library of a college or university’s film or media studies department and that are protected by technological measures that prevent their educational use.” Concluding that a “class” must be properly tailored not only to address the harm demonstrated, but also to limit the adverse consequences that may result from the creation of an exempted class, the Register has concluded that given the facts demonstrated by the film professor proponents of the exemption and the legitimate concerns expressed by the opponents of the proposed exemption, it makes sense that a class may, in appropriate cases, be additionally refined by reference to the particular type of use and/or user.<sup>44</sup>

This announcement departs significantly from prior rulemakings, in which the Register had concluded that Congress limited her authority to declaring classes of works without reference to classes of users.<sup>45</sup> Because the Register must consider each proposed exemption *de novo* every three years, however, the triennial revisiting also allows her to reassess the scope of her authority in light of the requested exemptions and the record made in their support. In the case of technologically protected films, the “works only” approach would have produced results that would have been overbroad had the exemption been granted, or underinclusive had it been denied. Defining the class as films in protected digital format would have opened all DVDs and access-protected videostreams or downloads to circumvention. But refusing any exemption would, according to the record the Register found persuasive, have frustrated specific non infringing educational uses of the films. Limiting the class definition to digitally-protected films in certain educational libraries might have been a half-way approach, for it would have addressed characteristics that go to the source of the protected copies of the work, rather than the nature of the work (as would, for example, a definition of the class of works as the 1940s Westerns) or the nature of the user. Although this narrowing avoids user-specificity, it still risks overbreadth, because access to the library is not necessarily limited to participants in the relevant course for which the educational use is to be made. Adding a user limitation to the place specification tailors the “class” to the non infringing uses the triennial rulemaking is designed to enable.

The current rulemaking exempts:

1. Audiovisual works included in the educational library of a college or

---

<sup>44</sup> Id. at 6-7.

<sup>45</sup> See Exemption to the Prohibition on Circumvention of Copyright Protection Systems for Access Control Technologies, 65 Fed. Reg. 64556, 64556, 64559 (proposed Oct. 27, 2000) (to be codified at 37 C.F.R. pt. 201); Exemption to Prohibition on Circumvention of Copyright Protection Systems for Access Control Technologies, 68 Fed. Reg. 62011, 62014-15 (Oct. 31, 2003) (to be codified at 37 C.F.R. pt. 201).

university's film or media studies department, when circumvention is accomplished for the purpose of making compilations of portions of those works for educational use in the classroom by media studies or film professors.

2. Computer programs and video games distributed in formats that have become obsolete and that require the original media or hardware as a condition of access, when circumvention is accomplished for the purpose of preservation or archival reproduction of published digital works by a library or archive. A format shall be considered obsolete if the machine or system necessary to render perceptible a work stored in that format is no longer manufactured or is no longer reasonably available in the commercial marketplace.

3. Computer programs protected by dongles that prevent access due to malfunction or damage and which are obsolete. A dongle shall be considered obsolete if it is no longer manufactured or if a replacement or repair is no longer reasonably available in the commercial marketplace.

4. Literary works distributed in ebook format when all existing ebook editions of the work (including digital text editions made available by authorized entities) contain access controls that prevent the enabling either of the book's read-aloud function or of screen readers that render the text into a specialized format.

5. Computer programs in the form of firmware that enable wireless telephone handsets to connect to a wireless telephone communication network, when circumvention is accomplished for the sole purpose of lawfully connecting to a wireless telephone communication network.

6. Sound recordings, and audiovisual works associated with those sound recordings, distributed in compact disc format and protected by technological protection measures that control access to lawfully purchased works and create or exploit security flaws or vulnerabilities that compromise the security of personal computers, when circumvention is accomplished solely for the purpose of good faith testing, investigating, or correcting such security flaws or vulnerabilities.<sup>46</sup>

The second, third and fourth classes are essentially carry-overs from previous rulemakings, which also listed certain classes of works whose obsolescent or malfunctioning technological protections impeded their lawful use.<sup>47</sup> The sixth class, albeit new, offers a variation on this theme (and may overlap with the § 1201(j) security-testing exception). The innovations appear in the first and fifth classes. We have seen that the Registrar's redefinition of 'class of works,' taking into account characteristics of the works' users, made the first exemption possible. It is conceivable that, in the future,

---

<sup>46</sup> 2006 Rulemaking, *supra* note 42, at 32-33. See also recommendation of the Register of Copyrights in RM 2005-11, Rulemaking on Exemptions from Prohibition on Circumvention of Copyright Protection Systems for Access Control Technologies, Recommendation of the Register of Copyrights (Nov. 17, 2006) [hereafter Recommendation] [http://www.copyright.gov/1201/docs/1201\\_recommendation.pdf](http://www.copyright.gov/1201/docs/1201_recommendation.pdf)

<sup>47</sup> See 2003 Rulemaking, *supra* note 44.

the Register will list additional user-defined classes when the beneficiary user group is discrete and can be articulated with similar precision. This may mean, for example, that access circumvention for other educational purposes might be permitted, so long as the persons entitled to circumvent, and the purposes for which circumvention is allowed, can be carefully controlled. While the current Rulemaking endorses film professors' circumvention of university-owned copies for the purpose of creating compilations of film clips for classroom use in film or media studies courses, (and one might imagine a similar exemption in the future, for example, for audio clips compiled by musicology professors for their classroom use), it is considerably less likely that the Register would announce a class of works consisting of all audio or audiovisual works circumvented for the general purpose of allowing members of the public to create "remixes" (even assuming these remixes were non infringing). The last example casts us back into the slough of overbreadth potentially vitiating the protection of access controls in the first place. But the need to limit user-defined classes to well-circumscribed (and thus controllable) sets of users may have the effect of confining the practice of certain fair uses to traditional fair use communities, such as library or university research and instructional staff, while excluding the population at large. As may be inferred from the specificity of the exceptions resulting from the triennial rulemakings, assisting the latter group's fair uses may be beyond the Register's statutory power to recommend; whether these broader goals may be achieved by other means remains to be seen.<sup>48</sup>

The fifth class of works, exempting "firmware that enable wireless telephone handsets to connect to a wireless telephone communication network," addresses a different kind of anti circumvention problem. The other exemptions and their predecessors arose in the context of a statutory scheme that was working as designed to protect works of authorship, where the design acknowledges the potential for encroachment on non infringing uses, and accordingly, through the triennial rulemaking process, builds in its own safeguards against inflexibility. The need for the cell phone exception arose because of arguable misuse of the anti circumvention protections to achieve a goal the statute was not designed to achieve. Like the producers of garage doors and printer cartridges in the *Chamberlain* and *Lexmark* cases, proprietors of wireless networks appear to be bootstrapping access to their network service to protection of the technological measure that controls access to the software which causes the cell phone to function in connection with the service.<sup>49</sup> The courts in the garage door and printer cartridge cases pierced through the veil of the access-controlled computer programs, correctly perceiving the commercial objective of the plaintiffs to be control over use of a utilitarian device, not

---

<sup>48</sup> See discussion *infra*, TAN 51-74.

<sup>49</sup> See Recommendation, *supra* note 45, at 48:

It was undisputed that mobile handset consumers who desire to use their handsets on a different telecommunications network are often precluded from doing so unless they can obtain access to the bootloader or operating system within the handset in order to direct the phone to a different carrier's network. The evidence demonstrated that most wireless telecommunications network providers do not allow a consumer to obtain such access in order to switch a cell phone from one network to another, and that the consumer could not use the cell phone with another carrier, even after fulfilling his or her contractual obligations with the carrier that sold the phone. In order to switch carriers, the consumer would have to purchase a new phone from a competing mobile telecommunications carrier.

control over enjoyment of copyrightable expression. A short answer to the cell phone service lock-up problem might therefore have been that the object of protection falls outside the scope of the DMCA, thus requiring no Copyright Office action because the access control is not protected against circumvention in the first place.

However, this reasoning falls short for cell phones. A cell phone operating system is complex software, which surely contains some minimally original expression that has not merged with its function (conditions perhaps not met in the printer and garage door cases). Therefore, it is a “work protected under this title,” whose associated access control may not be circumvented under § 1201(a)(1). In general, the more elaborate the computer program, the more a prohibition on circumventing a technological measure that controls access to that program seems consonant at least with the statutory text, albeit not at all with its purpose. As a result, Copyright Office intervention through declaration of an anti circumvention exception may have been needed to parry such attempts to leverage control over access to computer programs into control over use of utilitarian articles or services.

In concluding that “the software locks are access controls that adversely affect the ability of consumers to make noninfringing use of the software on their cellular phones,” the Register emphasized that

a review of the four factors enumerated in § 1201(a)(1)(C)(i)-(iv) supports the conclusion that an exemption is warranted. There is nothing in the record that suggests that the availability for use of copyrighted works would be adversely affected by permitting an exemption for software locks. Nor is there any reason to conclude that there would be any impact – positive or negative – on the availability for use of works for nonprofit archival, preservation, and educational purposes or on the ability to engage in criticism, comment, news reporting, teaching, scholarship, or research. Nor would circumvention of software locks to connect to alternative mobile telecommunications networks be likely to have any effect on the market for or value of copyrighted works. The reason that these four factors appears to be neutral is that in this case, the access controls do not appear to actually be deployed in order to protect the interests of the copyright owner or the value or integrity of the copyrighted work; rather, they are used by wireless carriers to limit the ability of subscribers to switch to other carriers, a business decision that has nothing whatsoever to do with the interests protected by copyright. And that, in turn, invokes the additional factor set forth in § 1201(a)(1)(C)(v): “such other factors as the Librarian considers appropriate.” When application of the prohibition on circumvention of access controls would offer no apparent benefit to the author or copyright owner in relation to the work to which access is controlled, but simply offers a benefit to a third party who may use § 1201 to control the use of hardware which, as is increasingly the case, may be operated in part through the use of computer software or firmware, an exemption may well be warranted. Such appears to be the case with respect to the software locks involved in the current proposal.<sup>50</sup>

---

<sup>50</sup> Id. at 52-53.

**Limited effect of rulemaking:** The triennial rulemaking thus offers the Copyright Office the opportunity to ascertain if device producers and service providers, by imposing technological measures to achieve goals that neither traditional copyright law nor the policies underlying the DMCA would permit, are overreaching, and accordingly recommend that the Librarian of Congress list “a particular class of copyrighted works” as to which the prohibition on circumvention will not apply. But if the rulemaking is a kind of safety valve, one should acknowledge that it may not let off enough steam. Two features of the statutory scheme constrain the Librarian’s ability to remedy device-makers’ misuse of technological measures. First, the statutory directive regarding “a particular class” indicates that the exempted works should be narrowly defined. Thus, while the Librarian may, on appropriate showing, list computer programs in individual devices whose access controls may be circumvented, it is not clear that Congress delegated the power to declare a “particular class” consisting of *all* devices whose technological measures control access to computer programs which in turn operate the device or service.

Second, and more importantly, even if the Librarian’s authority extends to such broad class identifications, the Librarian’s power is limited to suspending the prohibition on the act of circumvention; Congress has not concomitantly permitted the distribution of devices designed to circumvent the access controls on the listed works. In other words, the beneficiaries of the exemptions had better be able to neutralize the access control themselves; they will not find lawfully-marketed devices that will do it for them. Trafficking in devices remains prohibited, probably because a device that could be used to circumvent an access control on a listed class of works will remain equally capable of circumventing access controls on non listed classes. The inability of the device to tell the difference means either that all works will be vulnerable if the circumvention device may be distributed, or that non infringing uses of listed works will, for many, be difficult to achieve if the device is banned. Congress has drawn the line in favor of strong protection for technological measures, at the possible cost of some non infringing uses.

The same dog-wagging problem may not be present with regard to circumvention services. A person doing the circumvention can differentiate between, for example, unlocking a cell phone’s access code in order to allow the customer to use other wireless services and decrypting DVDs of current movies. Moreover, if the beneficiaries of the “particular class” exemptions may neither acquire a circumvention device, nor engage the services of a person competent to effect the circumvention, then listing the class may have little practical effect.<sup>51</sup> But the statute does not empower the Librarian to ensure that users in fact be able to perform the non infringing acts the class listing in theory enables. That assurance, if needed, must come from judicial interpretation of § 1201(a)(2)’s ban on trafficking in or marketing circumvention services in light of the purpose of the triennial rulemakings.

---

<sup>51</sup> For example, query whether the film professors at issue in the film clips exception would themselves be capable of circumventing the access controls. But for the purposes cited in the exception, perhaps the university’s or film studies department’s IT group would come within the scope of the permissible activity.

**Other authority for broader exemptions:** How much range does § 1201 give judges to interpret its provisions in light of its apparent purposes? The delegation to the Copyright Office to designate circumventable classes of works suggests that Congress intended administrative rather than judicial proceedings to afford the primary means of making the scheme more responsive to user needs not already specified in the statute. But, as we have seen, the triennial rulemakings have several shortcomings. Can one find in § 1201 the leeway to allow judges to do better?

Reference to statutory purpose may enable judges to interpret the anti trafficking ban flexibly in connection with services targeted to circumventing access controls on classes of works whose non infringing use the Librarian has found likely to be endangered. While the statute does not permit the Librarian to suspend application of § 1201(a)(2) to these works, a court adjudicating an action brought against a person rendering circumvention services should take into account the purpose of exempting classes of works in the first place. Suppose, for example, that a consumer obtains assistance unlocking her lawfully-acquired but defective copy of an ebook or video game that comes within the scope of the Librarian’s designated exceptions. If the ebook or game publisher pursued the repair service that accomplished the circumvention, a court should consider whether a finding of violation would frustrate the statutory goal of ensuring that non infringing uses remain available. Unless the court attributed to Congress the cynical motive of declaring a non infringing use-preserving policy while deliberately withholding the practical means to achieve it, the court should give effect to the announced objective. This solution is a modest call for flexibility consonant with the statutory goals; it does not mean that a court may ignore the ban on trafficking in devices or in circumvention services not targeted to listed classes of works. As to those prohibitions, there is a discernable statutory purpose that the listing of circumventable classes does not call into question.

In addition, might courts refine § 1201(a)(1)’s ban on circumventing a measure that “controls access to a work protected under this title” by more closely scrutinizing the technologically controlled work allegedly protected under Title 17? The *Lexmark* court distinguished between computer programs that are “conduits” to copyrighted works, such as the programs that cause video games to run, and programs that simply cause machines to run. But, despite its initial attractiveness, determining the protectability of a computer program based on the nature of the thing whose functions it controls is problematic. *All* computer programs make things work, but their copyright protection does not turn on whether the thing is a copyrighted work, such as electronic music, or a device that produces copyrighted works, such as a digital camera, or a machine that neither is nor generates a copyrighted work, such as a temperature and humidity-controlled wine cooler. If a third party copied the computer program that controls the wine cooler’s temperature and humidity settings, a defense that the program accomplishes utilitarian tasks would be unavailing (assuming the code met conditions of originality and non merger). An infringement action would address the expressiveness of the code, not the objectives of its output. As we have seen, once a protectable computer program is the object of the access control, the conditions for applying the anti circumvention rules are at least formally met, hence the Copyright Office’s apparent perception that it is limited

to address user interests through articulation of a triennial exception rather than by proclaiming that the statute does not apply in the first place.

But a court may have a freer hand. In interpreting “controls access to a work protected under this title,” a court mindful of the absence of legislative intent to protect useful articles and their aftermarkets might look past the admittedly protected computer program to focus on what the measure is *really* controlling access to.<sup>52</sup> One way to test the proposition that the real work or object in interest is not the computer program but the thing it controls would be to ascertain whether “a rose by any other name would smell as sweet”: if a function-controlling program by any other code would do the trick, then the access measure does not genuinely target the expression of the computer program but instead uses the program as the means to control the associated useful article. A court might thus see through the smokescreen of the program and hold the measure uncovered by § 1201(a). One may garner further support for this approach from § 1201(a)(1)(C), which articulates criteria for the Librarian to take into account in designating classes of works whose non infringing uses the ban on access circumvention jeopardizes. As the Register stressed in setting out her reasons for exempting the cell phone software locks,<sup>53</sup> all of the criteria assume that the access-protected work is expressive; it makes no sense to examine the availability of useful articles and services for "non profit preservation" (ii) or "criticism, comment, news reporting, etc." (iii) . A court might go the next step to determine that the criteria do not address the leveraging of computer programs to lock up non copyrightable useful articles or services, because under a proper reading of § 1201(a)(1)(A), such articles or services would be excluded from the scope of anti circumvention protection in the first place, and therefore any need for the Librarian triennially to exempt those programs from the circumvention ban would not arise.

If a court rules that the technological measure controls access to something that is not a protected work, then not only may the end user circumvent the measure, but she may resort to a service to engage in the circumvention; the § 1201(a)(2) anti trafficking prohibition applies only to services circumventing technological measures on protected works. (Of course, to avoid running afoul of § 1201(a)(2), the service must limit its activities to circumventing technological measures attached to non protected works.) By contrast, for the reasons explored earlier, the ban on trafficking in circumvention devices would continue to hold.

The cases and Rulemakings to date have presented straightforward examples of leveraging access control over a nominally copyrighted work into de facto control over utilitarian articles or services (printer cartridges, garage doors, cell phone networks). But one may envision a hybrid deployment of access controls, for example, as the Register’s Report in the latest Rulemaking evokes, a measure controlling access both to a cell phone

---

<sup>52</sup> Cf. *Lexmark*, *supra*, 387 F.3d at 552-53 (Merritt, J., concurring) (anticipating more “complex and creative” lock-out codes, and cautioning that these should not make an anti circumvention action any more successful; rather courts should guard against “[g]iving authors monopolies over manufactured goods” by “allow[ing] authors exclusive control over not only their own expression, but also over whatever functional use they can make of that expression in manufactured goods”).

<sup>53</sup> See discussion *supra*, TAN 49.

network and to copyrightable content on the cell phone, such as music and images.<sup>54</sup> The Register suggests that the measure should be disaggregated to distinguish controls on access to the network service from controls on access to the expressive works: “it appears that there is no reason why those other works cannot be protected by separate access controls . . . .”<sup>55</sup> The proposition merits generalization: Future attempts to bootstrap control over useful articles and services (DMCA misuse) to control over access to expressive works (appropriate applications of the DMCA) should invite exacting judicial and administrative scrutiny.

The same observation should also apply to hardware lock-ins. Consider the DRM Apple has employed on iTunes files: it controls both the number of devices to which the file may be copied, and prevents uploading to the Internet.<sup>56</sup> These are bona fide access (and copy) controls within the scope and contemplation of the DMCA. But the same DRM also prevents playing the file on a player that is not an iPod. There is no evidence that, in fostering new business models of digital delivery, Congress also intended to favor particular delivery-receiving *devices*. On the contrary, the legislative history suggests congressional solicitude for preserving competition among devices.<sup>57</sup> Assuming the goals of DMCA did not extend to locking consumers into particular hardware devices, one might inquire -- consistently with the current Rulemaking’s analysis of DRM that inappropriately bundles access to cell phone services with access to musical content stored on cell phones -- whether the DRM attached to iTunes files should distinguish between access to the works and access to the player. There is, admittedly, a distinction between the bundled DRM the Register’s report addressed and a hardware lock à la iTunes: the criticized cell phone DRM attaches to a computer program that controls the functions of a useful article (the phone), while the iTunes DRM attaches to the work of authorship. Unlike cell phones and such, musical compositions, sound recordings, and other works of authorship are the intended focus of the anticircumvention protections. Nonetheless, the distinction may ultimately be without a difference: the hybrid DRM the Register envisioned would also attach directly to the musical and other works stored in the cell phone’s memory. The problem arises not from the linking of DRM to the work of authorship, but from combining that link with one that controls access to devices. If content-DRM persists inseparable from hardware-DRM, perhaps the Librarian, in the next Rulemaking, should declare a class of works consisting of digital format musical works and audiovisual works whose access controls limit access to the work to particular playback devices. As a result, breaking the access code in order to make the files compatible with other players would be permissible.

---

<sup>54</sup> See Rulemaking, *supra* note 42 at 53.

<sup>55</sup> *Id.*

<sup>56</sup> Apple has recently announced that it would not employ this DRM on higher-priced EMI songs (though EMI recordings sold at the lower-price point will continue to include DRM). See Ethan Smith and Nick Winfield, EMI to Sell Music Without Anti-Copying Software --- Online-Strategy Shift Breaks With Industry on Combating Piracy, WALL STR. JR., Apr. 2, 2007, at B5.

<sup>57</sup> See 105<sup>th</sup> Congress, H.R. 2281, § 107(2)(d) (Secretary of Commerce to report on "the degree to which [DMCA] claims constitute a serious impediment to the development and production of competitive goods and services"). This provision was not, however, included in the final version of the DMCA, which emerged from the Judiciary Committee’s rather than the Commerce Committee’s draft.

On the Rulemaking calendar, however, it will be another three years before the Librarian may declare such an exempted class. Must law-abiding music consumers wait that long, or might other provisions of the DMCA allow circumvention for the purpose of obtaining music player compatibility? At first blush, the “reverse engineering” exception, §1201(f) might appear on point, given its goal of “achiev[ing] interoperability.” On closer examination, however, the goal of interoperability with other playback devices does not seem to conform to that provision’s conditions. Section 1201(f)(1) states: “Notwithstanding the provisions of subsection (a)(1)(A), a person who has lawfully obtained the right to use a copy of a computer program . . .” A music file is not a computer program. It is in digital format, but not all works expressed in 1s and 0s are “computer programs.” Access to the digital file may be controlled by a computer program, but the subject matter addressed by § 1201(f) is the computer program whose access is being controlled, not the computer program controlling access. The exception thus fails at the threshold.<sup>58</sup>

In the absence of a statutory or timely administrative exception, our consumer would be left asking the court to create an interoperability exception, perhaps on grounds of circumvention misuse. But the need for judge-made exceptions may transcend the misuse scenario. For example, if the access-protected work is a genuine work of authorship rather than a pretextual software intermediary, the work would now be an appropriate object of access control, but the risk of over-control may still remain, especially when listing exempted classes of works does not lift the bar on trafficking in devices and services. Similar concerns apply to the ban on trafficking in devices that circumvent copy controls. If we conclude from the overall structure and legislative history of § 1201 that Congress did not intend to subject the anti trafficking bans to a general fair use limitation that would exonerate at least some acts of circumvention that do not lead to infringement or would excuse the distribution of devices that could be put to non infringing use,<sup>59</sup> we should next ask if section 1201 is therefore in tension with constitutional protections for free speech interests. In the absence of fair use, does the First Amendment require either devising a “fair circumvention” privilege, or else invalidating section 1201 as an undue burden on protected speech?

**“Fair Circumvention”?** Some litigants have asserted the unconstitutionality of the US Copyright Act’s anti-circumvention provisions. They have contended that fair use is constitutionally mandated and that section 1201 “eliminates fair use.” As a result, Congress would not have power to preclude fair use defenses to circumvention. Alternatively, they have argued that section 1201 suppresses speech and therefore violates the First Amendment. Every court that has so far encountered these challenges has rejected them.<sup>60</sup> With regard to the First Amendment, courts have observed that computer programs are a form of speech, but they are also functional. To the extent the government regulates the software’s functional aspects, the law is “content neutral” as to

---

<sup>58</sup> See Report of the House Committee on Commerce, Rept. 105-551, H.R. 2281, at 43 (the reverse engineering exception “applies to computer programs as such,” not to measures that “control[] access to any work other than a computer program”).

<sup>59</sup> See, e.g., *Universal City Studios, Inc. v. Corley*, 273 F.3d 429, 443 (2d Cir. 2001).

<sup>60</sup> See *Universal City Studios, Inc. v. Corley*, 273 F.3d 429 (2d Cir. 2001); *U.S. v. Elcom*, 203 F.Supp. 2d 1111 (N.D. Cal. 2002); *321 Studios v. MGM*, 307 F.Supp. 2d 1085 (N.D. Cal. 2004).

the speech aspects. The law will not be considered to violate the First Amendment if the regulation advances a legitimate government interest and is reasonably tailored to achieve that purpose. Congress' interest was in promoting electronic commerce in copyrighted works, and Congress could legitimately seek to achieve this objective by making the distribution of circumvention devices unlawful.<sup>61</sup>

The fair use assertions fared no better. Even granting that fair use plays an important, First Amendment-friendly role in balancing the rights of copyright owners against subsequent speakers, the courts have uniformly spurned the “extravagant claim” that section 1201 “unconstitutionally ‘eliminates fair use.’”<sup>62</sup> The courts have observed that unprotected copies in non-digital media remained available for all the usual fair use purposes, including by means of analog copying. Although copying from protected media, such as DVDs, might be rendered more cumbersome, it was not completely foreclosed. The courts emphasized that “[f]air use has never been held to be a guarantee of access to copyrighted material in order to copy it by the fair user’s preferred technique or in the format of the original.”<sup>63</sup> And “Defendant has cited no authority which guarantees a fair user the right to the most technologically convenient way to engage in fair use. The existing authorities have rejected that argument.”<sup>64</sup>

The courts’ rather abrupt treatment of the question probably reflects the contexts in which the cases arose as much as any views of the merits of a claim of entitlement to maximally convenient fair use. The cases have involved entrepreneurs and intermediaries who distributed circumvention devices that were perceived to facilitate piracy of DVDs and e-books. None of these intermediaries claimed to be themselves engaging in fair use of the circumvented works, nor did they show that their customers in fact sought the devices primarily in order to engage in non-infringing uses of the playable copies of DVDs that the devices enabled. Fair use in these contexts seemed primarily pretextual.

But the concerns about convenience are not frivolous: at some point, particularly if analog or unprotected versions cease to be readily available, “inconvenient” may look more like “impossible.” Should such a dismal future appear more imminent, it may well be appropriate to reconsider the scope of the circumvention prohibitions. At that point, we might need to take up the Supreme Court’s suggestion in *Eldred v Ashcroft* that legislation strengthening copyright could call for closer first amendment examination if it altered the “traditional contours” that the idea/expression distinction and fair use doctrine have shaped for copyright.<sup>65</sup> If, notwithstanding statutory safeguards, § 1201 in fact precludes non infringing uses, then the anti circumvention provisions may well invite first amendment condemnation. Courts should, however, resort to more conciliatory alternatives before applying a constitutional knock-out. *Eldred*’s two contour-setting

---

61. See, e.g., *Corley*, 273 F.3d at 453-58; *Elcom*, 203 F.Supp. 2d at 1127-37.

62. *Corley*, 273 F.3d at 458.

63. *Id.* at 459.

64. *Elcom*, 203 F.Supp. 2d at 1131.

<sup>65</sup> *Eldred v Ashcroft*, 537 US 186, 221 (2003).

doctrines are, after all, judge-made.<sup>66</sup> In codifying the fair use doctrine, Congress expressly disclaimed intent to “freeze” its development, “especially during a period of rapid technological change . . . the courts must be free to adapt the doctrine to particular situations on a case by case basis.”<sup>67</sup>

Admittedly, in the quoted passage from the legislative history of the 1976 Copyright Act, Congress endorsed further judicial development of a fair use defense to *copyright* infringement. A fair use defense to what some have called the “*para-copyright*” claims against circumvention<sup>68</sup> was not then at issue. But “fair use” (or something like it) may be an intellectual property law concept that ranges more widely than copyright. For example, judges have devised a “nominative fair use” defense to trademarks infringement.<sup>69</sup> Significantly, Congress has recently endorsed judicial limit-setting in trademarks cases, while simultaneously strengthening trademarks protection. In the Trademark Dilution Revision Act of 2006,<sup>70</sup> Congress expanded trademarks law to protect famous marks, even in the absence of likelihood of confusion. Congress thus afforded famous marks a scope of coverage more akin to a property “right in gross” than the traditional protection limited to remedying likelihood of deception or confusion.<sup>71</sup> To defuse the potential conflict between invigorated trademarks and expressive interests, Congress set out broad “exclusions,” of which the first is “Any fair use, including a nominative or descriptive fair use, or facilitation of such fair use of a famous mark by another person . . .”<sup>72</sup> The language is striking, because the terms “fair use” and “nominative fair use,” though increasingly familiar from the caselaw,<sup>73</sup> do not elsewhere appear in the statute. Nor does “descriptive fair use” as such, although section 33(b)(4) provides a defense regarding “a term or device which is descriptive of and used fairly and

---

<sup>66</sup> Congress recognized this in the legislative history of the 1976 Act, which codified both doctrines (as §§ 102(b) and 107). See House Report 94-1476, at 57, 66. See also Alan Latman, Study No. 14: Fair Use of Copyrighted Works, in 1 Studies on Copyright 781 (Arthur Fisher Mem. Ed. 1963).

<sup>67</sup> H.R. Rep. No. 94-1476, 94th Cong., 2d Sess. 66 (1976).

<sup>68</sup> David Nimmer, A Riff on Fair Use in the Digital Millennium Copyright Act, 148 U. Pa. L. Rev. 673, 686 n. 66 (2000)(emphasis supplied); Dan L. Burk, Anticircumvention Misuse, 50 UCLA L. Rev. 1095 (2003); Daniel C. Higgs, Lexmark International, Inc. v. Static Control Components, Inc. & Chamberlain Group, Inc. v. Skylink Technologies, Inc.: The DMCA and Durable Goods Aftermarkets, 19 Berkeley Tech. L.J. 59, 63 (2004); Craig Joyce et al., Copyright Law § 1.03[A], at 947 (6th ed. 2003).

<sup>69</sup> Courts have entertained “nominative fair use” defenses to trademark infringement, and may be developing broader concepts of non-statutory but lawful unauthorized use of trademarks. See, e.g., *New Kids on the Block v. News Am. Publ'g*, 971 F. 2d 302 (9th Cir. 1992); see also *Playboy Enterprises, Inc. v. Welles*, 279 F3d 796 (9th Cir. 2002); see generally J. Thomas McCarthy, *Non-confusing Nominative Fair Use*, 4 McCarthy on Trademarks and Unfair Competition § 23:11 (4th ed.). In addition, one scholar has argued for extending the fair use doctrine to patent law. See Maureen O'Rourke, *Toward a Doctrine of Patent Fair Use*, 100 Colum. L. Rev. 1177 (2000); see also Lorelei Ritchie de Larena, *What Copyright Teaches Patent Law about “Fair Use” and Why Universities are Ignoring the Lesson*, 84 Or. L. Rev. 779 (2005).

<sup>70</sup> HR 683, 109<sup>th</sup> Cong., 2d sess. (2006), --- P.L. ---

<sup>71</sup> On the dilution claim and its contrast with traditional trademark norms, see generally, Robert G. Bone, *Hunting Goodwill: A History of the Concept of Goodwill in Trademark Law*, *forthcoming* Boston U. L. Rev., [http://papers.ssrn.com/sol3/papers.cfm?abstract\\_id=874788](http://papers.ssrn.com/sol3/papers.cfm?abstract_id=874788); Mark A. Lemley, *The Modern Lanham Act and the Death of Common Sense*, 108 Yale L. J. 1687 (1999). On dilution's less impressive record in the courts, see Clarisa Long, *Dilution*, 106 Colum. L. Rev. 1029 (2006).

<sup>72</sup> 15 U.S.C. § 1125(c)(3)(A).

<sup>73</sup> See, e.g., decisions cited *supra* note 66.

in good faith only to describe the goods or services of such party, or their geographic origin.”<sup>74</sup> In other words, Congress appears to have taken trademark fair use as a given, perhaps even as a kind of omnipresence brooding over many intellectual property rights. The statute does not purport to create fair use; it restates it, in very open-ended fashion.

The statute illustrates the kinds of uses that qualify as trademark fair uses, by providing that fair uses “includ[e] use in connection with –

- (i) advertising or promotion that permits consumers to compare goods or services, or
- (ii) identifying and parodying, criticizing, or commenting upon the famous mark owner or the goods or services of the famous mark owner.”<sup>75</sup>

Congress thus codified these fair use concepts, in less methodological detail than its codification of copyright fair use in § 107 of the 1976 Copyright Act, but in a manner which, with its two “includings,” beckons further judicial intervention. Moreover, while Congress has endorsed these judge-made limitations in the context of the Dilution Revision Act, it would seem that they remain equally pertinent in the traditional, confusion-based, trademark actions in which they originated. The 2006 Dilution amendments thus support the broader proposition that when an intellectual property right poses a risk of conflict with free expression, fair use may avoid the peril. Absent evidence that the expanded intellectual property right cannot coexist with free expression, courts should not introduce exceptions that eviscerate the statute, but recognition of the residual role of fair use in intellectual property law in general suggests that, in appropriate circumstances, courts may temper § 1201 with carefully-tailored fair use-equivalent limitations.<sup>76</sup>

#### IV. Conclusion: The Cons, and Some Pros, of Strengthening Copyright through Protecting Access and Copy Controls

Section 1201 poses risks of over-protection, misuse and unintended consequences, although the likelihood of copyright owner success in overreaching will largely depend on the flexibility the Librarian and courts import to the statute. But the statutory interpreter must avoid both the rocky shoals of literal readings that produce nonsensical results, and the whirlpool of judicial rewritings that deprive the statute of much of the effect that Congress did seek to achieve.<sup>77</sup> To date, “digital lock-up” persists in spectral guise, a grim, yet untranspired, anticipation. While courts must remain

---

<sup>74</sup> Id § 1115(b)(4).

<sup>75</sup> Id § 1125(3)(A)(i)(ii).

<sup>76</sup> For further development of the argument for a “fair circumvention” exception, see, e.g., Rob Kasunic Identifying and Preserving the Traditional Contours of Copyright, *forthcoming* 31 Colum. J. L. & Arts. (2007) (symposium on constitutional challenges to copyright); Jane C. Ginsburg, From Having Copies to Experiencing Works: The Development of an Access Right in U.S. Copyright Law, in Hugh Hansen, ed., US INTELLECTUAL PROPERTY LAW AND POLICY 38, 56-58 (Edward Elgar 2006) (suggesting “fair access” exception); Yijun Tian, Problems of Anti-Circumvention Rules in the DMCA & More Heterogeneous Solutions, 15 Fordham Intell. Prop. Media & Ent. L.J. 749, 779 (Spring 2005).

<sup>77</sup> Compare *Lexmark v. Static Control Components* 253 F.Supp. 2d 943 (E.D. Ky 2003), rev’d., 387 F.3d 522 (6th Cir. 2004) (holding that circumvention of access code in order to make printer-compatible ink cartridge violates § 1201(a)) with *Storage Technology Corp. v. Custom Hardware Engineering & Consulting, Inc.*, 421 F.3d 1307 (Fed. Cir. 2005) (limiting unlawful circumvention to those acts that “facilitate copyright infringement”).

vigilant that this ghost not take concrete form, they should also bear in mind the many new business models that protected digital rights management (DRM) measures enable, lest insecurity dampen the prospects for these models' development.

A few examples of new models of delivery of audio and audiovisual works may buttress the point. There are a variety of music-streaming services, including RealNetworks, whose early § 1201 action against a service seeking to convert the copy-protected streams into a downloadable format we examined earlier.<sup>78</sup> Additional examples of streaming-only services include Netflix' new video-on-demand service,<sup>79</sup> the Rhapsody subscription music service,<sup>80</sup> and a burgeoning number of internet radio services.<sup>81</sup> Several television producers have been offering ad-supported streaming videos of some of their shows.<sup>82</sup> Some entertainment companies have also begun producing made-for-streaming shows.<sup>83</sup>

Other copy- or access-protected services allow downloads, but limited as to number of copies permitted, number of plays authorized, or time allotted to listen or view.<sup>84</sup> iTunes offers one of the best-known and most successful copy-limited download schemes; following in its wake is Amazon's Unbox, which offers downloadable movies that can be viewed only with its proprietary viewing software.<sup>85</sup> Competing services such as Movielink and CinemaNow, the major Internet movies-on-demand services, have begun to allow users to burn a single DVD copy of each movie downloaded from the repertoire of older films.<sup>86</sup> In addition, there are time-loaded downloads, permitting the user to keep the file for some period of time, or requiring the user, once she has opened the file, to view it within a certain period. The experience for the user approximates a movie rental, but without having to go to the store to acquire or return the film.<sup>87</sup> A

---

<sup>78</sup> See supra note 26.

<sup>79</sup> See David Pogue, A Stream of Movies, Sort of Free, New York Times, January 25, 2007, [http://www.nytimes.com/2007/01/25/technology/25pogue.html?\\_r=1&oref=slogin](http://www.nytimes.com/2007/01/25/technology/25pogue.html?_r=1&oref=slogin)

<sup>80</sup> See <http://www.rhapsody.com/home.html>.

<sup>81</sup> See, e.g., Radio IO, <http://www.radioio.com/>, Sirius Internet, <http://www.sirius.com/servlet/ContentServer?pagename=Sirius/Page&c=FlexContent&cid=1158082415620>, and Pandora ([www.pandora.com](http://www.pandora.com)).

<sup>82</sup> See [nbc.com](http://nbc.com), [abc.com](http://abc.com), [television.aol.com/in2tv](http://television.aol.com/in2tv).

<sup>83</sup> See Michel Marriott, Nothing To Watch on TV? Streaming Video Appeals to Niche Audiences, N.Y. Times, Aug 6, 2007 (describing "Devil's Trade", 6-episode show shot by joint venture for internet).

<sup>84</sup> Some content owners are also cooperating with websites that let users download their content (protected by DRM) for free. The content owners hope to make their money based on ads, see, e.g., [www.spiralfrog.com](http://www.spiralfrog.com). Nor is DRM technology limited to audio or video files: E-book sellers such as [barnesandnoble.com](http://barnesandnoble.com) also use DRM.

<sup>85</sup> See <http://blogs.zdnet.com/BTL/?p=3577>.

<sup>86</sup> See Bill Rosenblatt, "Movielink and CinemaNow Add DVD Burning," DRM Watch, July 20, 2006, <http://www.drmwatch.com/ocr/article.php/3621401> (criticizing services for allowing users to make only one copy of internet-on-demand movies)

<sup>87</sup> For example, the Microsoft Xbox videogame system now offers content licensed from CBS, Warner Brothers, MTV, and Paramount; it will have 1,000 hours of content available by the end of the year. Customers pay \$1.99 for the right to watch a movie any time within a two-week window. Once a customer begins watching the movie, he will have 24 hours to finish watching. See "Xbox Live to offer TV downloads," BBC News, 7 November 2006, <http://news.bbc.co.uk/2/hi/technology/6124042.stm>. The BBC has tested iMP, software that allows users to request BBC programs interactively for watching or listening

service called Slingbox allows a user to log in anywhere in the world and watch streaming video transmitted from his home television. A user can watch on only one remote computer at a time and cannot record programs remotely.<sup>88</sup> Another evolving DRM model is advertising-supported, and allows limited peer-to-peer downloading. For example, the Qtrax peer-to-peer service will hold licenses from major and independent record labels, and proposes to allow users to listen to songs a pre-defined number of times for free, before having to purchase the songs.<sup>89</sup>

Nor are DRM protections the exclusive redoubt of the major “copyright industries.” While many individual authors and artists and independent producers may disseminate their works with no technological restrictions on access or copying, new DRM-related payment methods are also taking shape, thus enabling creators directly to reap the benefits of digital exploitation. For example, the Mindawn online music service sells both unprotected permanent downloads of recorded music posted by independent artists, and DRM-protected “demo files” -- conditional downloads that allow the prospective buyer to “play it in full up to 3 times, and then the local copy of the file will self-destruct.”<sup>90</sup> The Snocap service allows unsigned artists (and others) to create Snocap-powered virtual stores anywhere on the web that sell the artist’s music. The artist keeps as much as 51 cents per dollar sold, and Snocap’s license is non-exclusive, thus allowing artists to offer their works from multiple sites. Artists can choose whether or not to sell their music with technological protection measures; approximately half employ Microsoft’s DRM.<sup>91</sup> In our solicitude for preserving user privileges in technologically-protected copyrighted works, we should also keep in sight the promise these measures may hold for authors and artists, and in the long run, for their public as well.

---

on their computers. The DRM technology allows the BBC to set limits specifically for each show; some shows might reside on computers for only a day, others for two weeks. See Simon Perry, “More details of BBC iMP revealed - All content DRM'd,” Digital-Lifestyles.Info, 26 February 2004, [http://digital-lifestyles.info/display\\_page.asp?section=distribution&id=1009](http://digital-lifestyles.info/display_page.asp?section=distribution&id=1009).

<sup>88</sup> See Sling Media Press Release, “Sling Media Gives Consumers Their TV “Anywhere-Anytime” with the Slingbox,” (June 30, 2005), [http://us.slingmedia.com/object/io\\_1157566576257.html](http://us.slingmedia.com/object/io_1157566576257.html). A similar service is provided by bigeardigital, which lets people upload audio content and access it from different devices and in different places. See [www.bigeardigital.com](http://www.bigeardigital.com).

The flourishing new business of offering “ring tone” downloads also employs DRM, with audio files available for download to cell phones, but protected against further transfer to other cell phone users via the internet or other form of messaging. See, e.g., Infospace, Ringtones & Graphics, <http://www.infospaceinc.com/mobile/ringtonesgraphics.php>. For an explanation, see, Open Mobile Alliance, Digital Rights Management, Short Paper (December 2003), <http://www.openmobilealliance.org/docs/DRM%20Short%20Paper%20DEC%202003%20.pdf> (“forward lock prevents content from leaving device” prevents peer-to-peer distribution).

<sup>89</sup> See also Peter Lauria, Top Music Labels Back QTrax Swap Service, N.Y. Post, June 25, 2007. See Robert Levine, New Model for Sharing: Free Music With Ads, N.Y. Times, Apr. 23, 2007..

<sup>90</sup> See Mindawn Artists’ FAQ re “demo files”: “The user can play it in full up to 3 times, and then the local copy of the file will self-destruct. The file is not playable outside of our player software, and our player “knows” how many times it has been played.” <https://www.mindawn.com/artists.php>

<sup>91</sup> See <http://www.snocap.com/about/faq/>. Snocap appears to be successful; one report estimates that it lists over 3.3 million songs. See Dan Fost, Tech Chronicles, The S.F. Chronicle, March 21, 2007, at C3.