

WILL MERGING ACCESS CONTROLS AND RIGHTS CONTROLS UNDERMINE THE STRUCTURE OF ANTICIRCUMVENTION LAW?

By R. Anthony Reese[†]

ABSTRACT

Copyright owners are increasingly using technological measures, often referred to as “digital rights management” systems, to protect their works in digital formats. In 1998, Congress granted copyright owners legal remedies against the circumvention of such measures and against the suppliers of circumvention technologies. This Article considers how the complex structure of these legal protections might affect copyright owners’ choices of which technological measures to deploy. Because Congress provided stronger protection to measures controlling access to copyrighted works than it provided to measures controlling copyright owners’ rights in those works, copyright owners might prefer access controls to rights controls. In practice, however, copyright owners may be able to employ technological protection systems that incorporate both an access control and a rights control. So far, courts have treated such “merged” control measures as entitled to the legal protections afforded *both* access-control and rights-control measures. The Article next considers the impact on consumers of copyright owners’ use of merged control measures. Congress expressly provided less protection for rights controls in order to allow consumers to make noninfringing uses of copyrighted works in protected digital format. By protecting merged control measures as both access controls and rights controls, courts may undermine this congressional scheme for balancing protections for copyright owners and the public’s interest in noninfringing use. Finally, the Article explores possible responses to the potential threat posed by the deployment of merged control measures, including amending the legal protections for technological control measures to allow the circumven-

© 2003 R. Anthony Reese

[†] Assistant Professor, School of Law, The University of Texas at Austin. B.A., Yale University; J.D., Stanford Law School. I thank Graeme Dinwoodie, Paul Goldstein, and Christopher Leslie for comments on earlier drafts. I thank Beth Youngdale of the Tarlton Law Library for research assistance.

tion of a merged control measure where the post-circumvention use of the protected work is noninfringing.

I. INTRODUCTION

Copyright owners show increasing interest in using technological measures, often referred to as “digital rights management” (DRM) systems, to protect their works in digital formats and control access to and use of those works. In 1998, Congress added a new chapter to U.S. copyright law, Chapter 12 of Title 17,¹ providing copyright owners who use such technological control measures with legal remedies against the circumvention of those measures and against the suppliers of devices or technologies that accomplish such circumvention.

This Article considers how these new legal protections potentially impact copyright owners’ choices about the type of technological control measures to employ with their works. The type of control measures copyright owners choose will, of course, depend on a variety of factors in addition to the legal protections, including availability, effectiveness, cost, and consumer acceptance.² But at least in part, the nature and degree of legal protection available against circumvention will likely influence the choice of which control measures to adopt.

Part II looks at how the complex structure of legal protections in Chapter 12 might affect copyright owners’ choices. In particular, this Part examines the different legal protection afforded to the two types of technological control measures protected by the statute: access-control measures and rights-control measures. Because access controls may enjoy stronger protection under the statute than rights controls, copyright owners may prefer access controls to rights controls.

In practice, however, copyright owners may not need to choose between the different types of legal protections available. Copyright owners may instead be able to employ technological protection systems that incorporate both an access control and a rights control. So far, courts have treated such “merged” control measures as entitled to the legal protections of *both* access- and rights-control measures, even when the system was essentially directed only at preventing copying and distribution, rather

1. 17 U.S.C. §§ 1201-1205 (2000).

2. See, e.g., Pamela Samuelson, *Intellectual Property and the Digital Economy: Why the Anti-Circumvention Regulations Need to Be Revised*, 14 BERKELEY TECH. L.J. 519, 566 (1999) (“Competition among information providers may also affect the successful deployment of technical protection systems. If one information provider tightly locks up his content, a competing provider may see a business opportunity in supplying a less tightly restricted copy to customers who might otherwise buy from the first provider.”).

than at controlling access. If courts continue to treat merged control measures in this manner, copyright owners may have an incentive to use such merged controls in order to maximize their legal protection.

Part III considers the impact on consumers of copyright owners' use of merged control measures and the courts' strong protection of such control measures. Congress expressly provided less protection for rights controls in order to allow consumers to make noninfringing uses of copyrighted works in protected digital format, just as consumers have for centuries made noninfringing uses of copyrighted works in unprotected analog copies. By protecting merged control measures as both access controls and rights controls, courts may undermine this congressional purpose by preventing consumers from legally engaging in conduct with respect to merged control measures that would be legal with respect to rights-control measures.

The deployment of merged control measures thus poses a threat to the congressional scheme for balancing protections for copyright owners against the public's interest in noninfringing use. Part IV explores possible responses to this threat. One response is to amend Chapter 12's legal protections to allow the circumvention of a merged control measure where the circumventing party's post-circumvention use of the protected work is noninfringing. This Part further explores some of the implications of such a proposal. While exempting such circumvention might be possible by means of a rulemaking procedure provided for in the statute, congressional action is probably necessary.

II. LIKELY PRACTICAL IMPACT ON COPYRIGHT OWNERS OF THE DIFFERENT LEGAL PROTECTION FOR ACCESS CONTROLS AND RIGHTS CONTROLS

A. Contrasting Access Controls with Rights Controls

The anticircumvention provisions of Chapter 12 carefully distinguish between two types of technological protection measures: any measure that "effectively controls access to" a copyrighted work;³ and any measure that "effectively protects a right of a copyright owner" under U.S. copyright law.⁴ The scope of legal protection given to each type of technological control varies.⁵

3. 17 U.S.C. § 1201(a)(1)(A), (a)(2).

4. *Id.* § 1201(b)(1).

5. In the European Union, by contrast, "the same protection is granted to technologies controlling access and to technologies protecting rights (e.g. copy control technol-

1. *Access Controls Receive Greater Statutory Protection*

Both access-control and rights-control measures are protected against the manufacture and distribution of devices and technologies that circumvent the measures.⁶ The statute essentially makes no distinction between devices that circumvent access- or rights-control measures with respect to outlawing such circumvention technologies and devices.⁷ Thus, if a product or service is primarily designed or produced to circumvent an access control or a rights control, or has only limited commercially significant purpose or use other than to circumvent such a control, or is knowingly marketed for use in circumventing such a control, then the manufacture or distribution of the product or service is illegal.⁸

The distinction between access controls and rights controls becomes significant, though, for the second type of legal protection that Chapter 12 offers to technological protection measures. The statute in some cases bars the very act of circumventing a technological control. However, the ban applies only to acts of circumventing *access* controls⁹ and not *rights* controls. A person who circumvents an access-control measure violates § 1201(a)(1)(A) and is subject to the civil remedies of § 1203 (including statutory damages of up to \$2,500 per act).¹⁰ If the circumvention is done “willfully and for purposes of commercial advantage or private financial gain,” the circumventor is subject to the criminal provisions of § 1204 (including a fine of up to \$500,000 and up to five years in prison for a first offense).¹¹

ogy).” Maria Martin-Prat, *The Relationship Between Protection and Exceptions in the EU “Information Society” Directive*, in *ADJUNCTS AND ALTERNATIVES TO COPYRIGHT* 466 (Jane C. Ginsburg & June M. Besek eds., 2002).

6. The language of the bans is quite broad. The bans provide that no one shall “manufacture, import, offer to the public, provide, or otherwise traffic in any technology, product, service, device, component, or part thereof” that meets certain criteria. 17 U.S.C. § 1201(a)(2), (b).

7. Actually, while the basic prohibitions on manufacture of and trafficking in circumvention technologies make no distinction based on the type of control measure being circumvented, certain of the exceptions to those basic prohibitions on devices do distinguish between access controls and rights controls. *See infra* text accompanying notes 66-67.

8. 17 U.S.C. § 1201(a)(2), (b)(1).

9. *See id.* § 1201(a)(1)(A).

10. *Id.* § 1203(c) (establishing civil remedies for any injury caused “by a violation of section 1201 or 1202”). A plaintiff alleging a § 1201 violation can pursue either actual or statutory damages. *See id.*

11. *Id.* § 1204(a) (imposing criminal penalties for such violations of § 1201 or § 1202).

ANTICIRCUMVENTION LAW

On the other hand, a person who circumvents a rights-control measure does not commit any violation of § 1201, and is not subject to any remedies or penalties under § 1203 and § 1204.¹² Instead, such a circumventor is subject only to liability for copyright infringement under § 501(a).¹³ Such liability turns not on the fact that the person circumvented the rights control, but rather on ordinary principles of copyright law as applied to the actions the circumventor took after the circumvention. Did she engage in an act of reproduction, distribution, adaptation, or public performance or display reserved exclusively to the copyright owner under § 106? Was her act authorized by the copyright owner, either expressly or impliedly, or was it excused by one of the specific limitations on the copyright owner's rights contained in §§ 107 through 122 of the Copyright Act? The Senate Report on the DMCA, in explaining the absence of a ban on acts that circumvent rights-control measures, makes this clear:

It is anticipated that most acts of circumventing a technological copyright protection measure will occur in the course of conduct which itself implicates the copyright owners['] rights under title 17. This subsection is not intended in any way to enlarge or diminish those rights. Thus, for example, where a copy control technology is employed to prevent unauthorized reproduction of a work, the circumvention of that technology would not itself be actionable under 1201, but any reproduction of the work that is thereby facilitated would remain subject to the protections embodied in title 17.¹⁴

In many instances, of course, one who circumvents a rights control will not infringe the copyright owner's rights in violation of "the protections embodied in title 17." She may reproduce part of the work, but her reproduction may qualify as fair use or as consumer noncommercial making of a musical recording, both of which are not infringements.¹⁵ She may publicly display the work, but that display might be authorized because it is made to an audience located at the same place as the lawfully made

12. "Section 1201(b) . . . does not prohibit direct acts of circumvention; the technologically adept user thus faces no liability under that section." Jane C. Ginsburg, *Copyright Legislation for the "Digital Millennium"*, 23 COLUM.-VLA J.L. & ARTS 137, 143 (1999).

13. See 17 U.S.C. § 501(a).

14. S. REP. NO. 105-190, at 29 (1998).

15. See 17 U.S.C. § 107 (providing that fair use of copyrighted material does not constitute infringement); *id.* § 1008 (providing that no action may be brought under Title 17 based on noncommercial use by a consumer of an audio recording device to make musical recordings).

copy of the work from which the display was made.¹⁶ She may publicly perform the work in the course of face-to-face teaching activities in a classroom of a nonprofit educational institution, as allowed by copyright law.¹⁷ The wrongfulness of the circumventor's actions thus turns not on her act of circumventing a technological measure that protects a copyright owner's exclusive rights, but rather on whether her actions infringe upon those exclusive rights, as limited by statutory provisions and common law doctrines.

The additional protection offered against acts of circumventing access controls but not rights controls offers some incremental protection to copyright owners. Since acts circumventing access-control measures will often take place in private, they will be no more likely to be detected (or to result in enforcement efforts) than individuals' private acts of reproduction (such as home taping, CD burning, or photocopying) have been under modern copyright law.¹⁸ An individual who circumvents an access-control measure in order to watch in private her own copy of a film that is region-coded or time-limited in order to prevent its performance seems no more likely to be sued by a copyright owner for violating § 1201(a)(1)(A) than an individual who records a television broadcast of a motion picture in order to repeatedly view it later is likely to be sued for copyright infringement.¹⁹

16. *See id.* § 109(c). For an in-depth discussion of noninfringing public displays, see R. Anthony Reese, *The Public Display Right: The Copyright Act's Neglected Solution to the Controversy Over RAM "Copies"*, 2001 U. ILL. L. REV. 83, 86-92.

17. *See* 17 U.S.C. § 110(1).

18. *See, e.g.*, Glynn S. Lunney, Jr., *The Death of Copyright: Digital Technology, Private Copying, and the Digital Millennium Copyright Act*, 87 VA. L. REV. 813, 830 (2001) (noting that because "enforcing the [act] prohibition will require lawsuits against each individual user" of circumvention technology, the "prohibition will prove largely impractical to control widespread private copying"); Neil Weinstock Netanel, *Impose a Noncommercial Use Levy to Allow Free P2P File Sharing*, 17 HARV. J.L. & TECH. (forthcoming 2003) ("Merely fortifying DRM controls with a prohibition against individuals' circumvention would have left copyright holders facing much the same enforcement costs and public relations risks as suing individual infringers under traditional copyright law."); Samuelson, *supra* note 2, at 554-55 (noting that the initial executive branch proposal on circumvention contained no bar on any acts of circumvention and suggesting that the drafters may have believed that "it would be difficult to detect individual acts of circumvention, and as long as such acts were done on an isolated, individual basis (due to the unavailability of circumvention devices), the danger to copyright owners would be small").

19. Such recording would not qualify as fair-use "time shifting" allowed by *Sony*, since the practice approved there involved taping broadcast material in order to watch it at another time and then erasing it. *See Sony Corp. v. Universal City Studios, Inc.*, 464 U.S. 417, 423 (1984).

ANTICIRCUMVENTION LAW

In some cases, however, someone who circumvents an access control will go beyond a mere private act of circumvention and will engage in more detectable activities which could lead to enforcement of the circumvention ban. The circumventor might make copies of the work and distribute them to the public, or might transmit performances or displays of the work over computer networks using, for example, peer-to-peer software. In those instances, a copyright owner might well detect the circumventing party's public, post-circumvention uses of the work. For example, someone who acquires a digital copy of a film protected by an access control that allows viewing the film for any single twenty-four-hour period, and who then circumvents the access control after the twenty-four hour period in order to copy the film, is more likely to be detected if she posts the copy she made on a peer-to-peer network than if she simply views it in her own home. The circumventing party in such circumstances is, of course, liable for any infringements of the copyright owner's exclusive rights under § 106. In the course of investigating or litigating the infringement claim, however, the copyright owner might also uncover the pre-infringement circumvention of the access-control measure. That would permit the copyright owner to pursue an additional cause of action against the circumventor for violation of § 1201. The copyright owner would presumably be entitled to relief for the act of circumvention, particularly statutory damages and possible treble damages, in addition to the relief available for the copyright infringement. Thus, while copyright owners may not need the ban on acts of circumvention in order to have some legal recourse against those who both commit such acts *and* are likely to be detected doing so,²⁰ that ban does give copyright owners additional relief against such parties.²¹

20. In addition, there is no need to impose liability on acts of circumvention in order to impose secondary liability on those who contribute to acts of circumvention by providing equipment or technology to do so, since § 1201(a)(2) and § 1201(b) directly impose liability on those who supply such equipment. In the context of copyright infringement, on the other hand, prohibiting private and likely undetectable acts of reproduction, performance, or display may be necessary for the imposition of liability for contributory infringement on those who facilitate such private activities, given the general view that some act of direct copyright infringement must occur in order for one to be held liable for contributory infringement. *See id.* at 434-42; 2 PAUL GOLDSTEIN, COPYRIGHT § 6.3.2, at 6:44 (2d ed. 1996 & 2000 Supp.) (“Courts, including the United States Supreme Court, have universally held that, for a defendant to be contributorily or vicariously liable, a direct copyright infringement must have occurred.”).

21. *See* Thomas Vinje, *Copyright Imperilled?*, 1999 EUR. INTELL. PROP. REV. 192, 198 (“Where damages are awarded or penalties imposed for circumvention in addition to those available for copyright infringement, the addition of a prohibition on circumvention could provide a significant supplemental deterrent to copyright infringement.”).

In other instances, a party circumventing an access-control measure may face liability for her circumvention even though she is not liable for copyright infringement for her post-circumvention activities. For example, a person who circumvents a measure controlling access to a copyrighted work in order to engage in a fair use, such as creating a parody of the copyrighted work, and who then publicizes the parody, would not be liable under copyright law for making the parody available to the public. However, she may face liability under § 1201 because by making the parody publicly available she has revealed her act of circumvention.²² In this case, the copyright owner would not have a viable infringement claim against the circumventing party, since the circumventor's use of the copyrighted work qualifies as a fair use. However, having revealed (at least indirectly) her act of circumvention, the parodist is subject to suit for circumventing the access control to engage in her noninfringing, transformative copying and potentially liable at least for statutory damages of up to \$2,500 per circumventing act.²³ Thus, in such instances, the ban on circumventing access-control measures offers a copyright owner legal recourse against a user where copyright law itself might give no relief.

In sum, Chapter 12 “gives the greatest protection to copyright owners’ right to control access” because it “tolerates direct end-user circumvention of post-access anticopying measures, to a far greater extent than it does circumvention of access controls.”²⁴ The greater protection for access controls may have practical benefits for copyright owners adopting DRM measures. Where an act of circumvention is detectable, Chapter 12 offers copyright owners relief against circumventors that goes beyond any relief available for the copyright infringement and offers the only potential relief against circumventing parties whose post-circumvention activities do not amount to copyright infringement. Such relief is unavailable against those who circumvent rights controls, and therefore access controls are likely to prove more attractive to copyright owners.

22. While the public dissemination of the parody would not necessarily provide direct evidence of the circumvention, if the copyrighted work had been distributed only in protected formats, then the dissemination of the transformed copy of the work might offer circumstantial evidence of the act of circumvention, and discovery during litigation might confirm that such circumvention took place.

23. 17 U.S.C. § 1203(c)(3) (2000). Alternatively, the copyright owner could pursue her actual damages and any profits earned by the violator. *Id.* In addition, the circumventor could face the impoundment and destruction of any computer equipment used in her circumvention. *See id.* § 1203(b)(2), (6).

24. Ginsburg, *supra* note 12, at 139.

ANTICIRCUMVENTION LAW

2. *Courts May Interpret the Statute to Give Access Controls Greater Legal Protection Against Circumvention Devices*

Access controls receive greater protection under Chapter 12 than do rights controls, since only access controls are protected against acts of circumvention. But even with respect to the ban on disseminating circumvention technologies, which applies to both types of control measures, Chapter 12 may, depending on how courts interpret its language, offer stronger or more certain protection to access-control measures than to rights-control measures.

Any measure that effectively controls “access” to a work is protected under Chapter 12. The term “access” is never defined,²⁵ but is likely to be read broadly, probably extending to any act by which the work is made perceptible.²⁶ Thus, any measure that controls a user’s ability to perceive a work will likely qualify for protection under § 1201(a), and technologies circumventing any such control will be outlawed unless they have some other commercially significant purpose.

Technological control measures may have more difficulty qualifying for protection as rights-control measures, partly because a copyright owner’s rights are constrained by exceptions. A rights-control measure is one that effectively protects a right of a copyright owner under the Copyright Act. Although the copyright owner’s rights are quite broad, encompassing reproduction, distribution, adaptation, public performance, and public display,²⁷ they are nevertheless subject to numerous limitations and exemptions. First, the copyright owner’s rights extend only to public performances and displays; all private performances and displays are entirely outside the scope of the copyright owner’s rights.²⁸ So someone who plays

25. The statute does define when a technological measure “effectively controls access to a work” as “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.” 17 U.S.C. § 1201(a)(3)(B). This definition in no way narrows the concept of “access” protected by § 1201.

26. See Jane C. Ginsburg, *From Having Copies to Experiencing Works: The Development of an Access Right in U.S. Copyright Law*, in U.S. INTELLECTUAL PROPERTY 2 (Hugh Hansen ed., 2000), available at http://papers.ssrn.com/sol3/papers.cfm?abstract_id=222493 (“Every act of perception or of materialization of a digital copy requires a prior act of access.”); *id.* at 12 (“Thus, ‘access to the work’ becomes a repeated operation; each act of hearing the song or reading the document becomes an act of ‘access.’”); GOLDSTEIN, *supra* note 20, § 5.17.1, at 5:245 (“Access to a work in the sense evidently contemplated by section 1201(a) occurs any time a user derives value from a work without necessarily infringing one of the exclusive rights secured by copyright.”).

27. 17 U.S.C. § 106.

28. Indeed, not every work enjoys exclusive performance and/or display rights. Most significantly, sound recording copyright owners have no general exclusive right to

recorded music on CD or a film on DVD in the privacy of her own home is in no way exercising any right of the copyright owner. Second, the statutory grant of exclusive rights to copyright owners is subject to express exceptions.²⁹ Certain acts are outside the scope of the copyright owner's exclusive rights and are therefore not infringing, even though they are acts of reproduction, distribution, adaptation, public performance, or public display. For example, it is not copyright infringement for teachers or students of a nonprofit educational institution to perform a copyrighted work in a classroom in the course of face-to-face teaching activities,³⁰ even though the teacher or students would be performing the work "publicly" as the Copyright Act defines that term.³¹ As a result of the express exceptions, the rights of the copyright owner are not the very broadly stated exclusive rights of reproduction, adaptation, distribution, public performance, and public display. Instead, the copyright owner has the rights to reproduce, distribute, adapt, and publicly perform or display her work "exclusively" only to the extent that the statute does not expressly permit such activities by other people.

Technological protection measures that control reproduction or performance of a work, however, are unlikely to be well calibrated to the actual contours of, for example, copyright owners' reproduction or public performance rights.³² Consider a technological control measure on the performance of a motion picture in a format such as a DVD. Perhaps the control measure requires the user of the DVD to enter a code before the film can be performed, possibly a code unique to the DVD player on which the disc was first played, thus essentially "tethering" the particular disc to a

perform or display their works publicly. *Id.* §§ 106(4), 114(a). They do, however, have a narrow right to perform their works publicly by means of a digital audio transmission. *Id.* § 106(6).

29. 17 U.S.C. § 106 grants exclusive rights to copyright owners and is subject to exceptions provided in §§ 107-122.

30. *Id.* § 110(1).

31. *See id.* § 101 ("publicly"). That definition includes performing a work "at any place where a substantial number of persons outside of a normal circle of a family and its social acquaintances is gathered," which would probably be the case in many classroom settings. *Id.*

32. *See* Dan L. Burk & Julie E. Cohen, *Fair Use Infrastructure for Rights Management Systems*, 15 HARV. J.L. & TECH. 41, 55-57 (2001) ("At least for now, there is no feasible way to build rights management code that approximates both the individual results of judicial determinations and the overall dynamism of fair use jurisprudence."); Julie E. Cohen, *Some Reflections on Copyright Management Systems and Laws Designed to Protect Them*, 12 BERKELEY TECH. L.J. 161, 177 (1997) ("Automated [copyright management systems] are inherently ill-equipped to handle the equitable, fact-specific inquiry required in fair use cases.").

ANTICIRCUMVENTION LAW

particular player.³³ The control measure would most likely require entry of the code for *any* performance of the film, whether it is to be viewed by an individual in a private residence (a private performance entirely outside the scope of the § 106(4) right), by a class of students (a public performance, but one permitted under § 110(1)), or by an admission-paying audience in an auditorium (a public performance within the copyright owner's exclusive rights). In the case of the auditorium showing, the control measure effectively protects the copyright owner's rights by limiting the exercise of the public performance right under § 106(4). In the other two cases, however, the control measure does not limit the exercise of the copyright owner's public performance right. Instead, the measure controls the user's ability to engage in performances that are entirely noninfringing and outside the scope of the copyright owner's exclusive rights.³⁴ Is such a measure protected under § 1201(b)? Is it illegal to manufacture and distribute a device that circumvents such a control measure?

Section 1201(b) protects a technological control measure if the control “effectively protects a right of a copyright owner under [Title 17],” which means that “the 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.”³⁵ The tethering control effectively protects the copyright owner's public performance right—at least in cases where the user of the DVD performs the work publicly. After all, some of the activity controlled by the measure—e.g., showing the film to paying viewers in an auditorium—is within the copyright owner's rights. The difficulty, however, is that much of the activity controlled by the measure is *not* within those rights. But because the statute does not say that a control measure must *only* control against infringing activities, the tethering control may qualify as a control measure that effectively protects a right of the copyright owner.

It is not clear, though, that a device circumventing such a broadly targeted control measure would be prohibited under § 1201(b). That section

33. For a discussion of “tethered” copies, see R. Anthony Reese, *The First Sale Doctrine in the Era of Digital Networks*, 44 B.C.L. REV. (forthcoming May 2003); U.S. COPYRIGHT OFFICE, DMCA SECTION 104 REPORT 75 (2001), available at http://www.copyright.gov/reports/studies/dmca/dmca_study.html.

34. A measure preventing the copying of recorded music is another example of a measure that would limit a user's ability to engage both in conduct reserved to the copyright owner *and* conduct permitted to the user under Title 17. Section 106(1) gives copyright owners the exclusive right to reproduce musical works and sound recordings, but § 1008 allows a consumer to make “noncommercial” copies of recorded music. See 17 U.S.C. §§ 106(1), 1008.

35. *Id.* § 1201(b)(2)(B).

essentially outlaws circumvention technology if it is “primarily designed or produced for the purpose of,” or if it “has only limited commercially significant purpose or use other than,” circumventing the protection afforded by a rights-control measure.³⁶ What of a technology that enables a user to circumvent a copyright owner’s control measure where that measure prevents the user not from engaging in activity reserved to the copyright owner but in an entirely noninfringing activity, such as privately performing a motion picture? What of a device that allows a person to take a DVD “tethered” to her home DVD player and play it on a different DVD player in a friend’s home? Arguably, that device has the use of circumventing a technological measure that interferes with lawful activity—privately performing a copyrighted motion picture—rather than (or in addition to) circumventing a technological measure that protects a right of the copyright owner. If that use is of more than limited commercial significance, then the device might not be barred by § 1201(b)(1), which only outlaws devices that circumvent rights controls.³⁷

The statute might nevertheless be read to ban such a device. Section 1201(b)(1) outlaws technologies that circumvent “protection afforded by a technological measure that effectively protects a right of a copyright owner.”³⁸ Thus, for example, circumventing a tethering control in order to privately perform a copyrighted work might be considered circumventing “protection afforded by” a rights-control measure, even though that measure’s protection is not, in that instance, directed to a right of a copyright owner. Under this broad reading of the statute, as long as a control measure in *any* way protects a copyright owner’s rights *in addition to* controlling legitimate, noninfringing activities, then a technology’s ability to circumvent the measure in order to allow such legitimate, noninfringing activities would be irrelevant to determining whether the circumvention technology is lawful.

This broad reading might find support in the different language Congress used in the access-control and rights-control device bans. In § 1201(a), Congress banned devices that “circumvent a technological measure” that controls access to a work, while in § 1201(b), Congress banned devices that “circumvent *protection afforded by* a technological

36. *Id.* § 1201(b)(1)(A)-(B).

37. Because the bans in § 1201(b)(1) are cumulative, in order to be legal, the device must also not have been primarily designed or produced for circumvention nor be marketed for circumvention.

38. 17 U.S.C. § 1201(b)(1)(A)-(C).

ANTICIRCUMVENTION LAW

measure” that protects a right in a work.³⁹ This difference in terminology could reflect a congressional intention to provide broader protection in § 1201(b). Read this way, § 1201(b) would outlaw devices that circumvent any protection provided by a rights-control measure, even if the protection in that instance was not itself directed at activity within the scope of the copyright owner’s rights.

At least one court has treated § 1201(b) in this broad manner with respect to devices that could be used to circumvent a rights-control measure in order to engage in fair use of a protected work. *United States v. Elcom Ltd.*⁴⁰ involved a computer program that circumvented technological measures used by e-book reader software to prevent copying, printing, lending, and reading aloud of e-books.⁴¹ The court acknowledged that the defendant’s software enabled the lawful owner of an e-book to engage in noninfringing conduct, such as reading the e-book on a different computer than the one onto which it was originally downloaded or making a backup copy of the book.⁴² The court further acknowledged the problem with § 1201(b)’s definition of rights-control measures arising out of the fact that “the rights of a copyright owner are intertwined with the rights of others” because of the statutory exceptions to the copyright owner’s exclusive rights.⁴³ The court nonetheless held that all devices that circumvent rights control measures are prohibited by the statute, even if the circumvention is made in order to enable a fair use outside the scope of the copyright owner’s rights. The court stated that “all tools that enable circumvention of [rights controls] are banned, not merely those [rights controls] that prohibit infringement.”⁴⁴

Reading § 1201(b)’s device ban so broadly poses a number of interpretive difficulties, though. As to the apparently broader language of § 1201(b)’s device ban as compared to § 1201(a)’s ban, Congress actually defined the phrase “circumvent protection afforded by a technological measure” to mean “avoiding, bypassing, removing, deactivating, or otherwise impairing a *technological measure*,”⁴⁵ suggesting that Congress did not perceive any difference between circumventing a technological measure and circumventing the protection afforded by a technological measure.

39. *Id.* § 1201(b) (emphasis added). Compare, e.g., *id.* § 1201(a)(2)(A) with *id.* § 1201(b)(1)(A).

40. 203 F. Supp. 2d 1111 (N.D. Cal. 2002).

41. *See id.* at 1118.

42. *See id.* at 1118-19.

43. *Id.* at 1121.

44. *Id.* at 1124.

45. 17 U.S.C. § 1201(b)(2)(A).

And at the point in the legislative history when the distinction in phrasing and definition between § 1201(a) and § 1201(b) appeared,⁴⁶ no one seems to have expressly indicated that the distinction was designed to outlaw circumvention devices that allowed users to engage in legitimate, noninfringing activities.

Indeed, Congress may have used two different phrases simply to avoid confusion between the definitions of “circumvent” in the two subsections. Each phrase is expressly defined in its own subsection. The definition of “circumvent a technological measure” in § 1201(a) is more detailed, giving the examples of descrambling a scrambled work and decrypting an encrypted work, in addition to the more general list of avoiding, bypassing, removing, deactivating, or impairing a technological measure.⁴⁷ In contrast, the definition of “circumvent protection afforded by a technological measure” in § 1201(b) only provides the general list and not the specific examples.⁴⁸

Perhaps the most significant interpretive difficulty with reading § 1201(b) so broadly is that such a reading renders the statute’s elaborate distinction between rights controls and access controls largely, if not en-

46. The language of the device bans in § 1201(a)(2) and § 1201(b)(1), and the associated definitions, are virtually unchanged from the language in companion bills H.R. 2281, 105th Cong. (1997) and S. 1121, 105th Cong. (1997), the first bills introduced to implement the WIPO Copyright Treaty anticircumvention requirements. In the 104th Congress, the NII Copyright Protection Act of 1995, H.R. 2241, 104th Cong. (1995) and S. 1284, 104th Cong. (1995) contained the first proposed version of § 1201, but that one-paragraph version made no distinction between access controls and rights controls, did not outlaw any acts of circumvention, and did not include the language and definitions under discussion. Nevertheless, the drafters of the anticircumvention provisions of the NII Copyright Protection Act expressly indicated that circumvention devices that enabled noninfringing uses would not necessarily be prohibited:

The Working Group recognizes . . . that . . . certain uses of copyrighted works are not unlawful under the Copyright Act. Therefore, the proposed legislation prohibits only those devices or products, the primary purpose or effect of which is to circumvent such [technological protection] systems *without authority*. That authority may be granted by the copyright owner *or by limitations on the copyright owner’s rights under the Copyright Act*.

INFORMATION INFRASTRUCTURE TASK FORCE, INTELLECTUAL PROPERTY AND THE NATIONAL INFORMATION INFRASTRUCTURE: THE REPORT OF THE WORKING GROUP ON INTELLECTUAL PROPERTY RIGHTS 231 (1995) (second emphasis added). The drafters further stated that “if the circumvention device is primarily intended and used for legal purposes, such as fair use, the device would *not* violate the provision, because a device with such purposes and effects would fall under the ‘authorized by law’ exemption.” *Id.* (emphasis original).

47. 17 U.S.C. § 1201(a)(3)(A).

48. *Id.* § 1201(b)(2)(A).

tirely, superfluous. Under such a reading of the section, every access control would automatically be a rights control as well.

Access to a work stored in digital format requires the ability to perceive that work: to see the text, hear the recorded sound, and view the visual images. In the analog world, human beings in many cases can directly perceive a copyrighted work from an analog copy—the text of a literary work that is printed on a page of a book, or the image of a painting on a canvas. Digitally formatted works, though, can be perceived only by using a machine that converts the stored (and generally humanly imperceptible) data into images and/or sounds. A literary work on CD-ROM requires software and hardware to convert the data on the CD into readable text on a screen, just as a motion picture on DVD requires software and hardware to convert data on the disc into a series of related images and accompanying sounds. This process of converting digitally stored data into humanly perceptible images and sounds constitutes, in virtually all cases, the display or performance of the copyrighted work.⁴⁹ One displays a work whenever one “shows” a copy of the work using any device or process,⁵⁰ while any “rendering” of a work, or showing of its images in sequence, constitutes a performance.⁵¹

49. In addition, in the view of some courts and commentators, any access to digitally stored information will, with current technology, involve reproducing the work in a copy, an activity within the copyright owner’s exclusive § 106(1) right. In order for digitally stored data to be made visible or audible by a computer, the data must temporarily be stored in the computer’s random-access memory (“RAM”). Some courts and commentators hold that temporary RAM storage constitutes the making of a “copy” or “phonorecord” for copyright purposes, and thus violates the copyright owner’s reproduction right unless authorized or otherwise excused. *See, e.g.,* MAI Sys. Corp. v. Peak Computer, Inc., 991 F.2d 511, 518-521 (9th Cir. 1993). This view is sharply contested. *See, e.g.,* Reese, *supra* note 16, at 139 & n. 219. But if it is accepted, then any act of gaining access to a digitally stored work would involve an act of reproduction within the scope of the copyright owner’s rights.

50. *See* 17 U.S.C. § 101 (“display”); *see also* H.R. REP. NO. 94-1476, at 64 (1976) (“In addition to the direct showings of a copy of a work, ‘display’ would include . . . the showing of an image on a cathode ray tube, or similar viewing apparatus connected with any sort of information storage and retrieval system.”); Reese, *supra* note 16, at 86-88.

51. *See* 17 U.S.C. § 101 (“perform”); *see also* H.R. REP. NO. 94-1476, at 63 (1976). The House Report states:

[A]ny individual is performing whenever he or she plays a phonorecord embodying the performance A performance may be accomplished ‘either directly or by means of any device or process,’ including all kinds of equipment for reproducing or amplifying sounds or visual images, . . . any type of electronic retrieval system, and any other techniques or systems not yet in use or even invented.

Id.

As a result, any access to a digitally stored work involves performing or displaying the work. In many instances, the performance or display made in the course of obtaining access to the work does not infringe on the exclusive rights of the copyright owner. Many such performances and displays are not public, and are therefore outside a copyright owner's exclusive rights of public performance and display.⁵² As long as a user accesses the work in a place that is not open to the public, such as a home or hotel room, and where a substantial number of people is not gathered, the performance or display involved in accessing the work is not an act within the copyright owner's control.⁵³ Even displays in public places are outside the scope of the copyright owner's right, as long as the display is made from a lawfully made copy and the viewers are present in the same place as that copy.⁵⁴

Because accessing a digitally stored work requires performing or displaying that work, a technological protection measure that controls access to the work also controls the performance or display of that work. If § 1201(b) is read broadly so that a rights-control measure is protected against circumvention devices even when the measure is controlling performances or displays that are not within the copyright owner's rights, then a device that circumvents an access control is simultaneously a device that circumvents a rights control.⁵⁵ That reading would render the statute's careful distinctions between access controls and rights controls largely meaningless. For example, several statutory exemptions from the ban on devices that circumvent access controls would not, in practice, exempt any circumvention device, because even though such a device would be within an exemption from the access-control protections of

52. See 17 U.S.C. § 106(4)-(5).

53. *Id.* § 101 ("publicly"); see also *Columbia Pictures Indus., Inc. v. Professional Real Estate Investors, Inc.*, 866 F.2d 278, 281-82 (9th Cir. 1989) (holding that viewing film on rented videodisc in hotel room videodisc player did not constitute public performance of film). This assumes that the user is not obtaining the access to the work by means of a transmission communicated from some other place, as transmissions to the public of performances or displays constitute public performances or displays.

54. See 17 U.S.C. § 109(c); see also Reese, *supra* note 16, at 88-92. The public performance and display rights are also subject to a range of narrower, more specific exemptions, such as those allowing classroom performances and displays, and performances of nondramatic musical works in record stores. See 17 U.S.C. § 110(1), (7).

55. If the "RAM copy" doctrine, see *supra* note 49, is accepted, then a device that circumvents an access control will simultaneously be a device that circumvents a rights control because the device circumvents a control on the reproduction of the work by means of RAM storage, in addition to circumventing a control on the performance or display of the work.

ANTICIRCUMVENTION LAW

§ 1201(a)(2), the device would fall afoul of the rights-control protections of § 1201(b), to which the exemption does not apply.⁵⁶

The legislative history of one particular exception from the anticircumvention bans further suggests that Congress did not consider an act of simply viewing or listening to a work to be within the rights of the copyright owner that could legally be protected by a rights-control measure. Section 1201(h) provides that in determining whether a device is a prohibited access-control circumvention technology, a court may consider the extent to which the device is necessary for preventing access by minors to material on the Internet. The legislative history of this section makes clear that it covers a device “which circumvents a technological protection measure effectively controlling access to a copyrighted work solely in order to provide a parent with the information necessary to ascertain whether that material is appropriate for his or her child.”⁵⁷ The drafters’ careful explanation of the exemption’s applicability only to access-control measures and not rights-control measures is illuminating:

This provision is limited to the application of subsection (a) because the Committee does not anticipate that it would be necessary for parental empowerment tools to make copies of questionable material, or to distribute or perform it, in order to carry out their important function of assisting parents in guiding their children on the Internet. Accordingly, circumvention of copy controls, or of similar measures, should never be a necessary capability of a parental empowerment tool. By the same token, if a technology, product, service or device . . . (1) has the sole purpose of preventing the access of minors to certain materials on the Internet, and (2) . . . circumvents a technological protection measure that effectively controls access to a work as defined in subsection 1201(a)(3) only for the purpose of gaining access to the work . . . to ascertain whether it is suitable for a minor, but does not otherwise defeat any copy protection for that work, then that technology, product, service or device is only subject to challenge under subsection 1201(a)(2) and not subsection 1201(b). In such circumstances, no cause of action would lie under section 1201(b) and therefore limiting language would be unnecessary.⁵⁸

56. Two statutory exemptions allowing in certain circumstances the making and use of devices that circumvent access controls, but not rights controls, are discussed in text accompanying notes 67-70, *infra*.

57. S. REP. NO. 105-190, at 14 (1998).

58. *Id.*

In most cases, of course, a parent cannot “ascertain” whether a work is suitable for a minor without seeing or hearing that work, and making the work visible or audible is an act of performance or display. Nonetheless, the drafters quite clearly viewed a device that circumvents a control measure in order to make such a limited—and presumably private—performance or display as not within the scope of § 1201(b)’s ban on rights-control circumvention devices. This supports the view that a device that circumvents a technological control in order to allow uses of a work that are outside the control of the copyright owner, such as private performances or displays, is not a prohibited device under § 1201(b).

A prominent commentator, Professor Jane Ginsburg, has suggested that this more narrow reading of § 1201(b) may be what Congress intended, and that Congress offered broader protection under § 1201(a) specifically because of the narrowness of the protection of rights-control measures.⁵⁹ Professor Ginsburg considers the case of a consumer who has purchased a digital copy of a film protected by a technological measure that allows the film to be viewed only one time, and a device that allows the consumer to circumvent that measure and view the film repeatedly without any further payment to the copyright owner.⁶⁰ She notes that the consumer’s viewing of the film would likely be a private performance:

As a result, the user . . . might not contravene a “right of the copyright owner,” and § 1201(b)[’s ban on rights-control circumvention devices] might therefore be ineffective. By contrast, if each viewing is an act of “access” to the work, then, . . . [any unpaid viewings after the initial viewing would be achieved through] circumventing an access control, and would be in violation of § 1201(a).⁶¹

This suggests that Congress protected access-control measures at least in part because it believed that its protection for rights-control measures might not include controls that in part limit user activities outside the scope of the copyright owner’s rights, such as private performances or displays.

If this more narrow reading of § 1201(b) is adopted by the courts, or even as long as uncertainty exists about how that subsection’s anti-device provisions will be interpreted, copyright owners may see access-control measures as more desirable because of a greater degree of legal protection against circumvention devices. Section 1201(a) essentially outlaws de-

59. *See* Ginsburg, *supra* note 12.

60. *Id.* at 143.

61. *Id.*

ANTICIRCUMVENTION LAW

vices that circumvent technological measures that control “access” to a work, rather than controlling the rights of the copyright owner. “Access” to a work, however, is not a defined term of particular scope, unlike the copyright owner’s rights set forth in § 106. In addition, “access” to a work is not one of the rights granted in § 106, and is therefore not expressly limited by any of the provisions of §§ 107 through 122 as the § 106 rights are. While performing a film privately or in a classroom setting is entirely outside the scope of the copyright owner’s rights to which § 1201(b) is directed, gaining access to the film in order to make such a performance is nowhere removed by statute from the scope of the copyright owner’s ability to control access using measures protected by Chapter 12. Thus, as Professor Ginsburg noted:

[T]he “access” that section 1201(a) protects goes beyond traditional copyright prerogatives. Indeed, the text indicates that “access” is distinct from a “right of the copyright owner under this title.”

. . . .

. . . [I]n granting copyright owners a right to prevent circumvention of technological controls on “access,” Congress may in effect have extended copyright to cover “use” of works of authorship In theory, copyright does not reach “use”; it prohibits unauthorized reproduction, adaptation, distribution, and public performance or display Not all “uses” correspond to these acts. But because “access” is a prerequisite to “use,” by controlling the former, the copyright owner may well end up preventing or conditioning the latter.⁶²

62. *Id.* at 140, 143; *see also* Ginsburg, *supra* note 26, at 2 (“Every act of perception or of materialization of a digital copy requires a prior act of access. And if the copyright owner can control access, she can condition how a user apprehends the work, and whether a user may make any further copy.”). Ginsburg states:

[B]y purchasing [a] CD ROM, I have acquired lawful access to a *copy* of the work. . . . But I do not access “the work” until I have entered the password (from the correct computer). Thus, when the law bars circumvention of controls on access to the “work”, “access” becomes a repeated operation, whose controls will be substantially insulated from circumvention under the text of section 1201(a). I would therefore not be permitted to circumvent the access controls, even to perform acts that are lawful under the Copyright Act, such as using my copy in another computer or lending it to a friend

Ginsburg, *supra* note 12, at 140-41.

In keeping with this broad view of “access,” courts have so far refused to read § 1201 in a way that treats as legitimate the circumvention of an access-control measure for the purpose of gaining access to a work in order to make noninfringing use of that work. In *Universal City Studios, Inc. v. Reimerdes*,⁶³ a case involving a computer program allowing the copying of encrypted motion pictures in DVD format, the district court considered whether “the possibility of noninfringing fair use by someone who gains access to a protected copyrighted work through a circumvention technology distributed by the defendants saves the defendants from liability [for dissemination of an access-control circumvention device] under Section 1201.”⁶⁴ The court concluded that “nothing in Section 1201 . . . suggests” that result,⁶⁵ and held the defendants liable for violating § 1201(a)(2) by trafficking in a prohibited access-control circumvention device.

Chapter 12 may thus offer copyright owners more protection against circumvention technologies directed at access controls than at rights controls. At the very least, until the scope of protection available under § 1201(b) is clarified with respect to measures that control both uses reserved to the copyright owner and those uses that are entirely permitted by copyright law, copyright owners seeking the maximum legal protection available for their DRM technologies may have incentives to choose access-control measures over rights-control measures.

3. *Rights Controls Are Subject to Fewer Exemptions but the Practical Impact of Such Exemptions Is Unclear*

The anti-device provisions of Chapter 12 might be thought to offer somewhat stronger protection to rights controls than to access controls because the rights-control protections are subject to fewer express statutory exceptions. Chapter 12 provides several very detailed exemptions allowing development and employment of some circumvention technologies (and certain acts of circumvention). Two such exemptions apply to both access and rights controls.⁶⁶ But two other exemptions—those for encryp-

63. 111 F. Supp. 2d 294 (S.D.N.Y. 2000), *aff'd sub nom.* *Universal City Studios, Inc. v. Corley*, 273 F.3d 429 (2d Cir. 2001).

64. *Reimerdes*, 111 F. Supp. 2d at 323. While the court noted that the plaintiffs technically relied on both § 1201(a)(2) and § 1201(b)(1), the court’s discussion of this issue focuses entirely on the § 1201(a) claim.

65. *Id.*

66. 17 U.S.C. § 1201(e) (exemption for law enforcement activities; applicable to “[t]his section”); *id.* § 1201(f)(2) (exemption for reverse engineering computer program in order to achieve interoperability; allowing development and employment of technological means of circumvention “[n]otwithstanding the provisions of subsections (a)(2) and (b)”).

ANTICIRCUMVENTION LAW

tion research and security testing—expressly allow development and use of devices that circumvent access controls, but not rights controls.⁶⁷ The statute, therefore, allows a somewhat broader scope for producing devices that circumvent access controls rather than rights controls. Thus, a copyright owner seeking maximum legal protection against circumvention might prefer to use a rights control and thereby retain the ability to pursue legal action against the producer of a circumvention technology, even if that producer is engaged in otherwise statutorily acceptable encryption research or security testing.

It is unclear, however, whether allowing access-control circumvention devices for encryption research or security testing provides copyright owners with much practical incentive to prefer rights controls to access controls. The exceptions are quite narrowly defined.⁶⁸ The statute gives extremely detailed definitions as to what constitutes permissible encryption research and security testing and is designed to carefully limit the exemptions to persons engaged in those activities in good faith and not to others. In addition, the exemptions specifically prohibit any acts of security testing or encryption research that constitute copyright infringement.⁶⁹ Further, both exemptions fairly stringently limit the extent to which any circumvention technology developed for purposes of encryption testing or security research can be distributed to others.⁷⁰ Few devices or technologies are likely both to meet the exemptions' very specific standards and to

67. *Id.* § 1201(g)(4) (allowing development, use, and limited sharing of circumvention technologies “[n]otwithstanding the provisions of subsection (a)(2)”); *id.* § 1201(j)(4) (allowing development, production, distribution, or use of circumvention technologies “[n]otwithstanding the provisions of subsection (a)(2)”). Another provision that applies only to access controls, § 1201(h), discussed *supra* in text accompanying notes 57-58, is not actually an exemption, but rather a directive for a court to consider additional factors in determining whether a device is banned by § 1201 if the device includes a component that has the sole purpose of preventing access of minors to material on the internet. See Jonathan Band & Taro Issihiki, *The New Anti-Circumvention Provisions in the Copyright Act: A Flawed First Step*, CYBERSPACE LAW., Feb. 1999, at 2, 6; David Nimmer, *Puzzles of the Digital Millennium Copyright Act*, 46 J. COPR. SOC’Y 401, 408-409 (1999) (“This feature . . . in no way constitutes an exemption . . .”).

68. See, e.g., Ginsburg, *supra* note 12, at 151 (describing “the proliferation of narrow exceptions” and noting “the overspecification of special exemptions”); Samuelson, *supra* note 2, 537-39 (describing “seven very specific exceptions” as “narrowly crafted”).

69. 17 U.S.C. § 1201(g)(2)(D), (j)(2).

70. *Id.* § 1201(g)(4)(B) (allowing circumvention means to be provided “to another person with whom [the developer of those means] is working collaboratively for the purpose of conducting the acts of good faith encryption research”); *id.* § 1201(j)(4) (allowing distribution of circumvention means “for the sole purpose of performing the acts of security testing . . . provided such technological means does not otherwise violate section (a)(2)”).

be allowed to circulate freely under the exemptions. Given the relatively narrow scope of these exemptions to the ban on access-control circumvention devices, few copyright owners are likely to deploy rights-control measures, in whole or in part, out of a desire to avoid having their DRM technology subject to the exemptions.

B. Stronger Protection for Access Controls May Lead Owners to Prefer Them, Especially Since Access Controls May Easily Be Merged with Rights Controls

Because Chapter 12 protects access controls, but not rights controls, against acts of circumvention, and may offer access controls stronger protection against circumvention devices, copyright owners may have an incentive to prefer access controls over rights controls.⁷¹ However, copyright owners who use rights controls may nevertheless be able to enjoy the stronger protection given to access controls. Copyright owners may deploy technological controls that aim to limit users' ability to reproduce or disseminate copyrighted works but that implement those limits by joining a rights-control mechanism with an access-control mechanism. Courts might find such a "merged" access and rights control entitled to the protection of § 1201(a) and § 1201(b), thus freeing copyright owners of the need to choose between the two.

Of the very few cases so far decided under Chapter 12, at least two have involved such hybrid access-and-rights-control measures.⁷² The first,

71. Indeed, the Register of Copyrights described the original bill that eventually became Chapter 12 as "providing stronger protection" to access controls than to rights controls. *WIPO Copyright Treaties Implementation Act; and Online Copyright Liability Limitation Act: Hearing on H.R. 2281 and H.R. 2280 Before the Subcomm. on Courts and Intell. Prop. of the House Comm. on the Judiciary*, 105th Cong. 47 (1997) (statement of Marybeth Peters) [hereinafter Statement of Marybeth Peters].

72. At least eight cases involving claims under § 1201 have led to judicial opinions available in print or commercial electronic databases. See *Pearl Invs. LLC v. Std. I/O, Inc.*, Civ. No. 02-50-P-H, 2003 U.S. Dist. LEXIS 5376 (D. Me. Apr. 2, 2003); *Lexmark Int'l, Inc. v. Static Control Components, Inc.*, No. 02-571-KSF, 2003 U.S. Dist. LEXIS 3734 (E.D. Ky. Feb. 27, 2003); *Portionpac Chem. Corp. v. Sanitech Sys., Inc.*, 210 F. Supp. 2d 1302 (M.D. Fla. 2002) (claim dismissed for failure to state a claim; no facts given as to the nature of the control measure involved); *United States v. Elcom Ltd.*, 203 F. Supp. 2d 1111 (N.D. Cal. 2002); *CSC Holdings, Inc. v. Greenleaf Elecs., Inc.*, No. 99 C 7249, 2000 U.S. Dist. LEXIS 7675 (N.D. Ill. June 1, 2000) (cable TV descrambler prohibited by § 1201(a)(2) and by 47 U.S.C. § 553); *RealNetworks, Inc. v. Streambox, Inc.*, No. C99-2070P, 2000 U.S. Dist. LEXIS 1889 (W.D. Wash. January 18, 2000); *Universal City Studios, Inc. v. Reimerdes*, 111 F. Supp. 2d 294 (S.D.N.Y. 2000), *aff'd sub nom.* *Universal City Studios, Inc. v. Corley*, 273 F.3d 429 (2d Cir. 2001); *Sony Computer Entm't Am., Inc. v. GameMasters*, 87 F. Supp. 2d 976 (N.D. Cal. 1999). In addition, claims under the anticircumvention provisions were made, but not considered by the

ANTICIRCUMVENTION LAW

RealNetworks, Inc. v. Streambox, Inc.,⁷³ involved the plaintiff's "RealPlayer" software for receiving and performing streaming audio and video transmissions sent by computer servers using the company's RealServer" software.⁷⁴ A computer user who requested a transmission from a RealServer had to provide an authentication sequence, or "secret handshake," which was available only by using the RealPlayer software. By means of this authentication sequence, the transmitting RealServer would know that it was transmitting data to a RealPlayer and not to any other type of software.⁷⁵ All RealPlayer software, in turn, was designed to recognize and follow the instructions of the "copy switch" included in all RealServer transmissions. The copy switch indicated whether the receiving RealPlayer did or did not have permission to copy the transmitted audio or video by storing it, rather than simply playing the audio or video.⁷⁶ The defendant created a receiver for streaming transmissions, the Streambox VCR, that ignored the "copy switch" and allowed the user to record any received transmission. But in order for a Streambox VCR user to receive transmissions from a RealServer, the Streambox software had to provide the server with the "secret handshake" authentication sequence.⁷⁷

The court treated the "secret handshake" as an access-control mechanism and the "copy switch" as a rights-control mechanism, and found that Streambox's product circumvented both measures, violating § 1201(a)(2) and § 1201(b).⁷⁸ However, both the handshake and the switch clearly seem to have been parts of a single technological system designed to prevent the *copying* of streaming transmissions, rather than actually to restrict *access*

court, in *Sony Computer Entertainment, Inc. v. Connectix Corp.*, 48 F. Supp. 2d 1212, 1223 (N.D. Cal. 1999), *rev'd*, 203 F.3d 596 (9th Cir. 2000).

Indeed, one of the few pre-DMCA copyright cases to involve technological protection measures concerned a control that could be described as a merged access-rights control. *Vault Corp. v. Quaid Software Ltd.*, 847 F.2d 255 (5th Cir. 1988), involved the plaintiff's software "designed to prevent the unauthorized duplication of [computer] programs." *Id.* at 256. The plaintiff's system sought to prevent such copying (an activity potentially within the copyright owner's rights) by a system that required a software manufacturer's original diskette copy of the software to be present in a computer's drive in order for the computer to run the software. *See id.* Thus, access to the copyrighted work—the computer program—was allowed only from the original copy sold by the copyright owner. By limiting access in this way, the system would make unauthorized copying of the work futile.

73. No. C99-2070P, 2000 U.S. Dist. LEXIS 1889 (W.D. Wash. Jan. 18, 2000).

74. *Id.* at *5.

75. *Id.* at *6 (Finding of Fact 12).

76. *Id.* at *6-7 (Finding of Fact 13).

77. *Id.* at *10-12 (Findings of Fact 23-26).

78. *Id.* at *18-20 (Conclusions of Law 7-9).

to the transmitted work (except as necessary to restrict copying). In order to make the rights-control measure effective, the system was designed to allow access to the work only by software known to respect the rights-control technology.⁷⁹

The federal litigation over the software known as “DeCSS” and the technological protection used with DVD films provides an even clearer example of merged access and rights controls.⁸⁰ The case involved an encryption program, the “Content Scramble System,” or “CSS,” used by motion picture studios to protect films distributed on DVD, and a challenge to the DeCSS computer software that circumvented CSS. The trial court described CSS as follows:

CSS . . . is an access control and copy prevention system for DVDs developed by the motion picture companies It is an encryption-based system that requires the use of appropriately configured hardware such as a DVD player or a computer DVD drive to decrypt, unscramble and play back, but not copy, motion pictures on DVDs.⁸¹

CSS restricts copying of DVD films by joining an access-control measure with a rights-control measure. CSS allows a DVD film to be played, that is, accessed, only on a CSS-compliant player—the access-

79. RealNetworks may have been interested in limiting access for a reason other than controlling copying. Allowing a particular audio or video transmission to be heard or seen only using RealPlayer software may give consumers an incentive to acquire a copy of the RealPlayer software, thus increasing RealNetwork’s market share for media player software devices. As a practical matter, many transmitting entities make their audio or video files available in multiple formats so that users without RealPlayer software can hear or see the material using other software. It is not clear that copyright law, or “meta-copyright” law such as Chapter 12, should actively further a device-maker’s attempts to increase the market share for its device by restricting users’ ability to see or hear a copyrighted work on some other device. Indeed, copyright law has generally disfavored attempts by copyright owners of computer programs (such as RealPlayer) to use copyright law to limit the interoperability of their copyrighted computer programs with other computer programs or data. *See, e.g., Lotus Dev. Corp. v. Borland Int’l., Inc.*, 49 F.3d 807, 817-18 (1st Cir. 1995) (holding computer program’s menu command hierarchy an uncopyrightable method of operation based in part on concerns about program compatibility); *Sega Enters. Ltd. v. Accolade, Inc.*, 977 F.2d 1510, 1522-28 (9th Cir. 1992) (holding intermediate copying of a computer program as fair use where necessary to gain access to unprotected functional elements of program required for interoperability).

80. *Universal City Studios, Inc. v. Reimerdes*, 111 F. Supp. 2d 294 (S.D.N.Y. 2000).

81. *Id.* at 308.

ANTICIRCUMVENTION LAW

control measure.⁸² And CSS-compliant players only allow a DVD film to be seen, not copied—the rights-control measure.⁸³

As with the technology at issue in *RealNetworks*, CSS seems directed at controlling copying, not access. CSS imposes few actual limits on access,⁸⁴ in dramatic contrast to conventionally understood access-control measures, which impose far greater limits. For example, CSS does not tether playback of a particular copy of a film to a particular machine, thereby limiting access to the work to one particular DVD player. Similarly, CSS does not limit the time period in which a film can be viewed or the number of times it can be played. By contrast, the now-defunct Divx system typically allowed the owner of a copy of a film to play the film only on one system and only during one forty-eight-hour period, unless the user paid an additional fee for additional viewing.⁸⁵

The real concern addressed by CSS was preventing users from *copying* films stored on DVD and *disseminating* those copies⁸⁶—that is, from exercising exclusive rights of the copyright owners, the province of rights controls. As the trial court in the DeCSS litigation noted, “the principal

82. *See id.* at 310 (“[O]nly players and drives containing the appropriate keys are able to decrypt DVD files and thereby play movies stored on DVDs.”).

83. *Id.* (noting that CSS was licensed under strict security requirements “to ensure . . . that compliant devices could not be used to copy as well as merely play CSS-protected movies” and that CSS licensees “may not . . . make equipment that would supply digital output that could be used in copying protected DVDs”); *see also* Universal City Studios, Inc. v. Corley, 273 F.3d 429, 437 (2d Cir. 2001) (“With the [CSS] player keys and the algorithm, a DVD player can display the movie on a television or movie screen, but does not give a viewer the ability . . . to copy the movie.”).

84. The main access limit imposed by CSS, which the courts in the DeCSS federal litigation never discussed, is that a user cannot, in some instances, access a DVD that is coded for a region other than the region of the user’s DVD player. *See* Exemption to Prohibition on Circumvention of Copyright Protection Systems for Access Control Technologies, 65 Fed. Reg. 64,556, 64,569 (Oct. 27, 2000) (final rule adopting exemptions from ban on acts circumventing access controls under § 1201(a)(1)(C)). Even this limit, though, is quite weak, as multi-region DVD players are available which allow the viewing of DVDs coded for different regions, as are players set to single, but non-U.S., region codes. *Id.*

85. The Divx system operated so that once a user began playback of a Divx disc, the disc could be played back only for a limited time (e.g., forty-eight hours) and only on players registered to the same billing account. In order to view the disc again, or on a different player, the user’s player would have to contact the issuer of the disc and pay for additional access. *See, e.g.,* R. J. Dunill, *The Origins of the Original Divx*, at <http://www.techtv.com/screensavers/answerstips/story/0,24330,3368584,00.html> (modified Jan. 18, 2000).

86. Dissemination might be by distribution of copies of the film or by transmission of the film over computer networks such as the Internet, to recipients who could either view the transmitting performance or record a copy of the transmission.

focus of [the studios'] concern [over DeCSS] . . . is the transmission of pirated copies over the Internet or other networks."⁸⁷ The only real control that CSS placed on access was that users could access DVD films only on a CSS-compliant player, and the only reason to limit access to CSS-compliant players appears to be that those players prevented users from copying the films. Motion picture copyright owners seem to have little or no interest in restricting a user from *performing* a DVD film on a non-CSS-compliant player. As long as the user plays a lawfully made DVD, the device on which she performs the film has no effect on the copyright owner.⁸⁸ The studios' real concern was to keep the user from using such a device to *copy* the film.⁸⁹

CSS thus appears to be quintessentially a technological measure designed to protect rights of the copyright owner to reproduce and disseminate the film on a DVD. This control over the exercise of rights was implemented, however, by limiting access to the film only to certain devices. CSS allows a DVD to be played only on a licensed player, and licensed players do not provide digital output that can be copied.⁹⁰ Thus, the goal of limiting a user's ability to copy was achieved in part by restricting the user's ability to access the work by allowing access only on certain authorized devices. As a result, CSS could be seen as both a rights-control and an access-control measure within the definitions of Chapter 12, although in fact CSS primarily limits the reproduction of the protected work, rather than access to it.

The structure of merged access and rights controls seen in the DeCSS and *RealNetworks* cases is likely to be used in the design of any "trusted system" that restricts a user's ability to copy (or distribute, perform, or dis-

87. *Universal City Studios, Inc. v. Reimerdes*, 111 F. Supp. 2d 294, 314 (S.D.N.Y. 2000); *see also* *Universal City Studios, Inc. v. Corley*, 273 F.3d 429, 436 (2d Cir. 2001) (noting that digital format carries risk that virtually perfect copies can be easily made and disseminated and that CSS was a response to this risk of increased piracy); *Reimerdes*, 111 F. Supp. 2d at 309 (noting film studios' concern that DVD technology carried "an increased risk of piracy by virtue of the fact that digital files . . . can be copied without degradation from generation to generation"); *id.* at 315 (noting "two major implications" of DeCSS for studios, both stemming from ability of DeCSS users to reproduce and disseminate CSS-protected films); *id.* at 341-42 (discussing injury to plaintiffs from circulation of DeCSS and focusing on harm from use of DeCSS to make unauthorized copies).

88. *See Corley*, 273 F.3d at 453 ("The initial use of DeCSS to gain access to a DVD movie creates no loss to movie producers because the initial user must purchase the DVD.").

89. *See id.* ("However, once the DVD is purchased, DeCSS enables the initial user to copy the movie in digital form and transmit it instantly in virtually limitless quantity, thereby depriving the movie producer of sales.").

90. *See supra* note 83.

ANTICIRCUMVENTION LAW

play) copyrighted material. A trusted system consists of “hardware and software that can be relied on to follow certain rules [that] specify the cost and a series of terms and conditions under which a digital work can be used.”⁹¹ Key to a trusted system is that a work intended for restricted use is encoded “in such a way that it can be displayed or printed only by trusted machines.”⁹² Thus, a copyright owner who uses a trusted system to control a user’s ability to exercise rights reserved to the copyright owner will use both an access control—technology allowing the user to view, hear, store, or print the work only on compliant devices—and a rights control—technology in those compliant devices restricting the user’s copying, performance, etc., of the work. Therefore when using such trusted systems, copyright owners could be seen as using both an access-control measure *and* a rights-control measure.

If a merged access and rights control such as a trusted system is viewed by courts as both an access and a rights control, copyright owners using such a system may simultaneously enjoy the different legal protections afforded to each type. The DeCSS litigation suggests precisely this outcome. Although the copyright owners were concerned about DeCSS because of its potential to allow users to make copies of films stored on DVD (and to transmit those copies over computer networks), the district court ruled based on its legal analysis that DeCSS was a prohibited device for circumventing an *access* control, not based on an analysis of DeCSS as a technology for circumventing a copy control.⁹³ This is not to say that the result in *Reimerdes* would have been any different if the court had analyzed CSS as a rights control, rather than an access control. After all, the *device* bans of § 1201 are virtually identical, so that a device that circum-

91. Mark Stefik, *Trusted Systems*, SCI. AM., March 1997, at 79; *see also* COMPUTER SCI. & TELECOMM. BD., NAT’L RESEARCH COUNCIL, *THE DIGITAL DILEMMA* 167-71 (2000).

92. Stefik, *supra* note 91, at 79; *see also id.* at 80 (describing transaction on trusted system to acquire a digital copy of a book and noting that “[t]he entire transaction . . . is preceded by an exchange of information in which the seller ensures that [the buyer’s] machine is a trusted system”); Mark Stefik, *Shifting the Possible: How Trusted Systems and Digital Property Rights Challenge Us to Rethink Digital Publishing*, 12 BERKELEY TECH. L.J. 137, 139-40 (1997) (describing that before online trusted-system transaction can take place between distributor and consumer, “the two systems—the consumer’s system and the distributor’s system—need to establish that they are both trusted systems”); Mark Stefik & Alex Silverman, *The Bit and the Pendulum: Balancing the Interests of Stakeholders in Digital Publishing*, COMPUTER LAW., Jan. 1999, at 1, 4 (“Trusted systems . . . exchange copies of the work only with systems that can prove themselves trusted via challenge-response protocols.”).

93. *See* *Universal City Studios, Inc. v. Reimerdes*, 111 F. Supp. 2d 294, 316-24 (S.D.N.Y. 2000).

vents a trusted system seems likely in many cases to be prohibited, whether it is viewed as a device to circumvent an access-control or a rights-control measure. Indeed, it is quite likely that the courts would have found DeCSS to be a rights-control circumvention technology prohibited under § 1201(b)(1) and provided the same relief to the plaintiffs. But by basing their decisions about a control measure directed at preventing copying and dissemination almost wholly on the grounds that DeCSS was an improper access-control circumvention device, the courts' decisions suggest that trusted systems and similar merged access and rights controls will enjoy both the statutory protections given to rights controls *and* the apparently stronger protections afforded access controls where the treatment of the two types differs, such as for acts of circumvention.

This approach to merged control measures is not necessarily dictated by the statute. While the *RealNetworks* and *Reimerdes* courts viewed merged technological controls as constituting an access control protected under § 1201, a future court might read the definition of an access-control measure to exclude merged access and rights controls that in fact serve principally to control reproduction and dissemination, rather than access. The key phrase in this reading of the definition of a protected access-control measure is that the measure must control access "in the ordinary course of its operation."⁹⁴ As the Register of Copyrights noted in testimony to Congress, this definition would not cover "every technological measure that controls access."⁹⁵ Rather, the "'ordinary course of its operation' [language] would exclude technologies that may have the incidental or unintended effect of controlling access, or do so only when used in an unusual way."⁹⁶ Thus, a court might decide that the *RealNetworks* and *CSS* technological protection systems control access only incidentally because their control over access is merely incidental to the systems' control over a user's ability to reproduce protected works. Nonetheless, given the decisions to date interpreting Chapter 12, and the tendency of the courts rendering those decisions to read the statute fairly broadly, it is more likely that courts will continue to consider the access-control portion of a merged access and rights control to constitute an access control protected against circumvention by § 1201(a).

Copyright owners interested in controlling the exercise of their rights under § 106 may thus have incentives to deploy merged technological measures. These merged measures would control a user's activities in part

94. 17 U.S.C. § 1201(a)(3)(B) (2000).

95. Statement of Marybeth Peters, *supra* note 71, at 47.

96. *Id.* (commenting on definitional language in its initial appearance in introduced legislation).

by allowing access to the work only via certain devices. These devices would then restrict the user's ability to copy, disseminate, perform, or display the work. By doing this, the copyright owner would be able to protect the technological measure as both an access control *and* a rights control. Since access controls, as discussed above, enjoy stronger protection than rights controls under Chapter 12, copyright owners seeking maximum protection for their rights-controlling technological protection systems might well decide to deploy merged controls.

III. IMPACT ON USERS OF COPYRIGHTED WORKS IF COPYRIGHT OWNERS DEPLOY MERGED CONTROL MEASURES

As suggested in Part II, copyright owners may adopt DRM technologies that restrict *copying* by limiting *access* to authorized devices, so that the technology simultaneously qualifies both as an access control and a rights control. This use of merged access and rights controls, may, however, undermine Chapter 12's carefully differentiated treatment of the two types of controls. Understanding why this result is problematic requires understanding why the statute allows circumvention of rights-control measures in the first place.

Congress chose not to prohibit circumvention of rights-control measures in order to accommodate copyright owners' need to protect against infringement of their works in digital format and the need to allow the public to continue to make noninfringing uses of copyrighted works.⁹⁷ This emerges very clearly in the Register of Copyright's statement to Congress evaluating the initial draft of the provisions that eventually became Chapter 12.⁹⁸ The Register pointed out how the bill would accommodate the public's ability to engage in noninfringing uses.⁹⁹

97. See *United States v. Elcom Ltd.*, 203 F. Supp. 2d 1111, 1120 (N.D. Cal. 2002) ("Congress did not prohibit the act of circumvention [of rights controls] because it sought to preserve the fair use rights of persons who had lawfully acquired a work."); Band & Issihiki, *supra* note 67, at 3 ("The Administration [while formulating its legislative proposal for the anticircumvention bill] eliminated [a draft ban on acts of circumventing rights controls] in response to the library and education communities' concerns about the negative impact of the legislation on fair use."); David Nimmer, *Appreciating Legislative History: The Sweet and Sour Spots of the DMCA's Commentary*, 23 CARDOZO L. REV. 909, 932, 984-85 (2002) (noting that structure of § 1201 allows § 1201(b) to encompass fair use).

98. See Statement of Marybeth Peters, *supra* note 71.

99. While there are substantial differences between the bill about which the Register testified and the full text of Chapter 12, the enacted law made few if any changes to the fundamental features contained in the initial bill, particularly in the definitions of the

The Copyright Office firmly believes that the fair use doctrine is a fundamental element of the copyright law, and that its continuing role in striking an appropriate balance of rights and exceptions should not be diminished. We also believe that it is possible to provide effective protection against circumvention without undermining this goal.

Section 1201 seeks to accomplish this result in several ways. First, it treats access-prevention technology separately from infringement-prevention technology, and does not contain a prohibition against individual acts of circumvention of the latter. As a result, an individual would not be able to circumvent in order to gain unauthorized access to a work, but would be able to do so in order to make a fair use of a work which she has lawfully acquired.¹⁰⁰

Register Peters' last sentence is repeated almost verbatim in the House Judiciary Committee's report on the DMCA.¹⁰¹ The Copyright Office has officially expressed the same view on the enacted Chapter 12, stating, "The decision not to prohibit the conduct of circumventing [rights] controls was made, in part, because it would penalize some noninfringing conduct, such as fair use."¹⁰²

The Chair of the House Judiciary's subcommittee on intellectual property, Rep. Howard Coble—an initial sponsor of the anticircumvention legislation and a guiding force in its adoption—echoed these views in a letter to two colleagues, Rep. Tom Campbell and Rep. Rick Boucher, introduced into the *Congressional Record* during the floor debate leading to initial

measures protected, the prohibitions imposed, and the structure of differentiating between access controls and rights controls and not barring acts of circumvention of the latter. *See* Band & Issihiki, *supra* note 67, at 3 (noting that the basic framework of initial 1997 administration proposals of § 1201 "endures in the legislation enacted by Congress"); Nimmer, *supra* note 97, at 921 (noting that initial bill's "tripartite scheme survived through enactment").

100. Statement of Marybeth Peters, *supra* note 71, at 49. Register Peters noted that she was using "fair use" to refer collectively to "all permitted uses under the Copyright Act, including those made possible by the idea-expression dichotomy and the first sale doctrine." *Id.* at 48, n.1.

101. *See* H.R. REP. NO. 105-551, pt. 1, at 18 (1998) ("[A]n individual would not be able to circumvent in order to gain unauthorized access to a work, but would be able to do so in order to make fair use of a work which he or she has acquired lawfully.").

102. Exemption to Prohibition on Circumvention of Copyright Protection Systems for Access Control Technologies, 65 Fed. Reg. 64,556, 64,557 (Oct. 27, 2000).

ANTICIRCUMVENTION LAW

House passage of the anticircumvention provisions.¹⁰³ Campbell and Boucher had introduced a competing bill that they asserted better balanced copyright owners' needs for protection with the public interest in noninfringing uses.¹⁰⁴ Coble's letter explains his belief that the provisions eventually adopted as Chapter 12 offer substantial protection for noninfringing uses, and points principally to the lack of a ban on acts of circumventing rights-control measures as a key safeguard for such uses:

As it was introduced, H.R. 2281 contained two important safeguards for fair use. First, the bill dealt separately with technological measures that prevent access and technological measures that prevent copying. As to the latter, the bill contained no prohibition on the act of circumvention itself, leaving users free to circumvent such measures in order to make fair use copies.¹⁰⁵

Again, the absence of penalties for circumventing rights-control measures was recognized as a key feature of the legislation and as a mechanism for preserving fair use and other noninfringing uses of copyrighted works.

Thus, as Professor Pam Samuelson has concluded, “[t]he text of the DMCA and its legislative history clearly demonstrate that Congress intended to ensure that users would continue to enjoy a wide range of noninfringing uses of copyrighted works, even if copyright owners used techni-

103. This version passed in the House did not differ in any relevant respect from the bill approved by the Senate, and from the bill produced by the conference committee and enacted by Congress.

104. H.R. 3048, 105th Cong. (1997).

105. 144 CONG. REC. H7096-98 (daily ed. Aug. 4, 1998) (letter of Rep. Coble, Chair, Subcomm. on Courts and Intellectual Prop., House Judiciary Comm., to Rep. Campbell and Rep. Boucher (June 16, 1988)); *see also* H.R. REP. NO. 105-551, pt. 1, at 18 (1998). The Report states:

Paragraph (a)(1) does not apply to the subsequent actions of a person once he or she has obtained authorized access to a copy of a work protected under Title 17, even if such actions involve circumvention of additional forms of technological protection measures. In a fact situation where the access is authorized, the traditional defenses to copyright infringement, including fair use, would be fully applicable. So, an individual would not be able to circumvent in order to gain unauthorized access to a work, but would be able to do so in order to make fair use of a work which he or she has acquired lawfully.

Id. The second safeguard Coble pointed to was § 1201(c), which provides that nothing in § 1201 “shall affect rights, remedies, limitations, or defenses to copyright infringement, including fair use, under this title.” 144 CONG. REC. H7097 (daily ed. Aug. 4, 1998) (letter of Rep. Coble, Chair, Subcomm. on Courts and Intellectual Prop., House Judiciary Comm., to Rep. Campbell and Rep. Boucher (June 16, 1988)).

cal protection systems to impede them.”¹⁰⁶ One of the principal ways Congress implemented that intent was by expressly declining to prohibit acts that circumvent rights-control measures. Instead, Congress left regulation of that activity to the provisions of copyright law, which target only infringing activity.

In this context, both the deployment of merged access and rights controls and courts’ treatment of such a merged control measure as protected simultaneously under § 1201(a) and § 1201(b) raise troubling questions about the statute’s ability to preserve noninfringing uses of technologically protected works by not banning the act of circumventing a rights control. Users facing merged access and rights controls may be unable to circumvent the rights control (an entirely legal activity if the user’s post-circumvention use is not infringing) without circumventing the access control (a prohibited activity).¹⁰⁷ As a practical matter, then, the deployment of merged controls may restrict or eliminate users’ ability to legally circumvent rights controls. This undercuts the congressional intent in drafting the DMCA expressly to allow circumvention of rights controls so long as the circumventor does not engage in copyright infringement. If merged control measures are widely adopted, and if circumventing a merged control is treated as circumventing an access control, such treatment will suck most of the oxygen out of Chapter 12’s breathing space for

106. Samuelson, *supra* note 2, at 546.

107. Perhaps not all circumvention of a merged control will require circumvention of both the access-control and rights-control aspects of the system. Users might, for example, access the work on an “approved” or “trusted” device (e.g., an actual RealPlayer computer program, or a CSS-compliant DVD player), but adjust that device so that it does not respect the rights-control rules that it would ordinarily implement. A court might well find, though, that accessing a work on an altered device constitutes circumvention of an access control. For example, a court might find that CSS restricts access to CSS-compliant players, and that a DVD player that was CSS-compliant when produced by the manufacturer but that has been altered to allow the recording of digital output is no longer a CSS-compliant device. As a result, gaining access to a DVD film using the altered player could be considered circumventing the access-control aspect of CSS just as much as gaining access to the film using a player that was noncompliant *ab initio* would be. Even if such a process were not considered as circumvention of an access control, merged controls may still be problematic for the goal of allowing noninfringing circumvention. Given the limited number of users likely to be technologically sophisticated enough to engage in acts of circumvention without a device provided by someone else, it is not clear that Chapter 12 should make noninfringing circumvention more difficult by prohibiting the user from engaging in one likely avenue of circumvention, in this case the possibility of deceiving the control system into believing that the user’s device will comply with the system’s rights-control rules.

ANTICIRCUMVENTION LAW

circumvention of rights-control measures for noninfringing purposes.¹⁰⁸ As Professor Pam Samuelson suggests in a related context, “this presents the question of whether Congress should be understood to have made an empty promise of fair use and other privileged circumvention.”¹⁰⁹

The Copyright Office noted this problem in its first rulemaking on exemptions from the circumvention ban, stating that “[t]he merger of technological measures that protect access and copying does not appear to have been anticipated by Congress.”¹¹⁰ The Office pointed out that “the merger of access and use controls would effectively bootstrap the legal prohibition against circumvention of access controls to include copy controls and thereby prevent a user from making otherwise noninfringing uses of lawfully acquired copies.”¹¹¹ Therefore, the Copyright Office said, “the implementation of merged technological measures arguably would undermine Congress’s decision to offer disparate treatment for access controls and use controls in section 1201.”¹¹²

If copyright owners deploy merged control measures, and if courts protect those controls as both access and rights controls, then the freedom that Chapter 12 allows for circumventing rights controls will not, in fact, be the freedom to make noninfringing uses of technologically protected works as Congress intended it to be. A more careful treatment of merged controls under Chapter 12 is required.

108. The impact of merged controls might be less significant if courts interpret Chapter 12’s anticircumvention provisions to allow some circumvention of access controls in order for the circumventor to make fair use or other noninfringing use of the protected work. Both Pam Samuelson and Jane Ginsburg have suggested that the statute should be so interpreted. See Jane C. Ginsburg, *Copyright Use and Excuse on the Internet*, 24 COLUM.-VLA J.L. & THE ARTS 1, 8-9 (2000) (“[O]ne might conclude that courts may—given an appropriate fact situation—apply [the fair use doctrine] to § 1201(a) by articulating additional, and highly contextual, limitations on the prohibition on circumvention of access controls.”); Samuelson, *supra* note 2, at 539-40, 545-46. So far, however, courts have generally not followed this interpretive path, at least with respect to Chapter 12’s device bans. See *United States v. Elcom Ltd.*, 203 F. Supp. 2d 1111, 1123-25 (N.D. Cal. 2002); *Universal City Studios, Inc. v. Reimerdes*, 111 F. Supp. 2d 294, 322-24 (S.D.N.Y. 2000) (finding no fair use limitation on anticircumvention provisions). *But see RealNetworks, Inc. v. Streambox, Inc.*, 2000 U.S. Dist. LEXIS 1889 (W.D. Wash. 2000) (finding no fair use on the facts of the case, but not rejecting the possibility of fair use out of hand).

109. Samuelson, *supra* note 2, at 557.

110. Exemption to Prohibition on Circumvention of Copyright Protection Systems for Access Control Technologies, 65 Fed. Reg. 64,556, 64,568 (Oct. 27, 2000) (also noting that “neither the language of section 1201 nor the legislative history addresses the possibility of access controls that also restrict use”).

111. *Id.*

112. *Id.*

IV. POSSIBLE RESPONSES

Part II suggested that § 1201 may give copyright owners an incentive to adopt DRM systems combining an access control with a rights control, in an attempt to secure the maximum legal protection possible for their system. Part III suggested that such merged control measures, at least as they have been treated to date by courts applying § 1201, undermine a critical congressional goal behind that section: permitting some circumvention of technological protection systems to allow noninfringing uses. This Part considers what responses might be appropriate.

A. Do Nothing

Perhaps the likely deployment of merged access and rights controls requires no response. One reason why no response might be needed is that users may continue to be able to make noninfringing uses of copyrighted works in analog format. Many copyrighted works today continue to be widely available in both protected digital and unprotected analog formats, so that those who wish to make noninfringing uses of the work can do so by acquiring an unprotected analog copy. Motion pictures, for example, are today often available both on DVD, protected by CSS, and on videocassette, unprotected by CSS, perhaps alleviating some concerns about the difficulty a consumer might have in circumventing CSS to engage in noninfringing use of a film that she owns on DVD. In addition, even with protected digital copies, copying of the work may be possible when it is made audible or visible. As the Second Circuit noted in *Corley*, a user could play a film on a CSS-protected DVD and “recor[d] portions of the video images and sounds . . . by pointing a camera, a camcorder, or microphone at a monitor as it displays the DVD movie.”¹¹³ But relying on analog copying to preserve consumers’ ability to make noninfringing uses raises several problems. In the case of many works, copyright owners may well be moving toward issuing works only in protected formats, ending the availability of new works in unprotected analog copies. And while the possibility of copying the visual or audio output of a protected work may offer some room for noninfringing use, it seems likely as a practical matter to substantially diminish the quality and availability of such use. In addition, some copyright owners have expressed a desire to use technology, perhaps backed by legal requirements, to “plug the analog hole” and prevent such copying of copyrighted works.¹¹⁴

113. *Universal City Studios, Inc. v. Corley*, 273 F.3d 429, 459 (2d Cir. 2001).

114. *See, e.g.*, Motion Picture Ass’n of Am., *Content Protection Status Report*, at 9, at http://judiciary.senate.gov/special/content_protection.pdf (Apr. 25, 2002).

ANTICIRCUMVENTION LAW

A more significant reason why merged access and rights controls might not require any adjustment of Chapter 12's legal protections is that the law already prohibits circumvention devices for both types of controls. The main difference in the regulation of access and rights controls, which merged control measures threaten to blur, is that the statute bans only *acts* that circumvent access-control measures. Circumvention *devices*, on the other hand, are equally prohibited, regardless of which type of control measure they circumvent. As a result, the ban on acts of circumvention may be relatively unimportant as a practical matter, as all of the "action" may involve circumvention devices, for several reasons.¹¹⁵

First, any circumvention of most effective access controls will likely require technological ability beyond that of the average copyright consumer.¹¹⁶ Few DVD owners can defeat CSS on their own, without a device supplied by someone of greater technical skill.¹¹⁷ One court even suggested that Congress intended "to leave technologically unsophisticated persons who wish to make fair use of encrypted copyrighted works with-

115. As Pam Samuelson has noted, "the anti-device provisions are, as a practical matter, by far the more important rules." Samuelson, *supra* note 2, at 554; *see also* Yochai Benkler, *Free As the Air to Common Use: First Amendment Constraints on Enclosure of the Public Domain*, 74 N.Y.U. L. REV. 354, 416 (1999).

116. *See, e.g.*, Benkler, *supra* note 115, at 416 ("Even if a few savvy users can circumvent without relying on the products or services of others, the vast majority of users will have to rely on such products or services."); David Nimmer, *A Riff on Fair Use in the Digital Millennium Copyright Act*, 148 U. PA. L. REV. 673, 733, 739-40 (2000) (noting that "users . . . who lack technical expertise . . . are effectively checkmated" by Chapter 12's statutory scheme); Samuelson, *supra* note 2, at 551 ("It is unclear whether Congress intended for the technologically savvy who could 'do it themselves' to be the only ones who could engage in privileged acts of circumvention."). On the other hand, some protection systems *might* be easily circumvented. One protection system for recorded music distributed on CD in Europe was designed to prevent the CD from being played in a computer, as opposed to a single-purpose music CD player, such as a Discman or a stereo component, thus limiting access to certain types of devices. Reportedly, however, the protection system could be defeated by drawing a line with a black magic marker on the surface of the disc around the outer edge. If the access control qualified as "effectively" protecting access and thus covered by § 1201(a), even the technologically unsophisticated would be able to circumvent the access control in violation of § 1201(a)(1), though again copyright owners would seem unlikely to be able to detect any significant number of instances of prohibited circumvention.

117. Indeed, even with the source code for various programs to defeat CSS circulating fairly freely in a variety of forms, including on t-shirts and business cards, most consumers seem unlikely to be able to use that source code to actually decrypt and copy a film on a DVD. *See also* Benkler, *supra* note 115, at 416 (noting that barring circumvention technologies will "by and large negate the possibility of circumvention" as effectively as barring sale of VCRs would prevent most home copying of television broadcasts).

out the technical means of doing so.”¹¹⁸ Second, as noted above,¹¹⁹ even if an ordinary consumer obtains a circumvention device, any of her private acts of circumvention not resulting in subsequent—and independently actionable—acts of copyright infringement are unlikely to come to the attention of a copyright owner and result in enforcement efforts against her. On the whole, so few people may be able to circumvent access controls without the aid of prohibited circumvention technologies, and so few uses of those prohibited technologies are likely to be detectable, that copyright owners may get almost all of the practical protection they need and want from the device bans. Indeed, during the process leading to the enactment of Chapter 12, copyright owners strongly resisted proposals to adopt only a ban on acts of circumvention, arguing that they needed protection against the circulation of devices because of the difficulty of enforcing an act ban.¹²⁰

For most consumers, then, the absence of a ban on the circumvention of rights-control measures is of little or no practical import. Most users do not have the technological know-how to engage in legal circumvention of a rights control without the assistance of a circumvention technology. But because the device ban of § 1201(b) prohibits the manufacture and distribution of such circumvention technologies, few consumers will likely obtain circumvention technologies.¹²¹ Therefore, few consumers will be able

118. *Universal City Studios, Inc. v. Reimerdes*, 111 F. Supp. 2d 294, 324 (S.D.N.Y. 2000); *see also* Nimmer, *supra* note 116, at 739 (arguing that Congress’s failure to allow the technologically unskilled noninfringing circumventor to acquire circumvention technology “seems to be a conscious contraction of user rights”).

119. *See supra* notes 18-20 and accompanying text.

120. *See, e.g.*, Band & Issihiki, *supra* note 67, at 3-4 (noting copyright owners’ resistance to alternative legislative proposal that focused only on acts of circumvention, not devices, because of fear that anticircumvention ban would be too difficult to enforce if devices were available to consumers); Samuelson, *supra* note 2, at 554-56 (noting that administration proposals focused on device bans from the beginning and that proponents testified before Congress that anti-device provisions were “needed to stop deliberate and systematic piracy by ‘black box’ providers”).

121. A consumer capable of building her own circumvention device might not, however, violate the device ban in doing so. Section 1201 does not allow anyone to “manufacture, import, offer to the public, provide, or otherwise traffic in” any prohibited circumvention technology. 17 U.S.C. § 1201(a)(2), (b)(1) (2000). Provided that the device builder uses the device only for her own acts of circumvention, she would not be offering the device to the public or providing or otherwise trafficking in it, and if she builds it herself in the U.S., she would not be importing it. Thus, the only liability she might face would be for the “manufacture” of the device. But if she makes only the device or devices she needs for her own use, she arguably is not engaged in the “manufacture” of the device. While “manufacture” does mean to make a finished product, it typically means to do so in some quantity. I might build a bookshelf for my home, or sew several shirts to

ANTICIRCUMVENTION LAW

to engage in noninfringing acts of circumvention, even though the copyright law allows such acts. While a copyright owner's use of a merged control may interfere with a consumer's ability to legally circumvent the rights-control portion of the merged control, this interference will have little practical impact, since so few consumers will be able to engage in legal circumvention of rights controls in any event. From this perspective, deployment of merged access and rights controls and enforcement of the ban on acts that circumvent access controls will not practically hinder many legal acts of circumventing rights controls, because there may be few such acts.

In some instances, though, acts that circumvent merged control measures may not require illegal circumvention devices¹²² and may come to the attention of copyright owners through subsequent acts of the circumventor. In some instances the circumventing party will not have committed any subsequent act of copyright infringement, because her use of the work at issue was allowed by copyright law.¹²³ One example is someone who circumvents a technological control measure in order to copy parts of a work to make a parody or other noninfringing transformative fair use. The copier is not liable for copyright infringement for her copying, nor is she liable for circumventing a rights-control measure in order to make the

wear, or bake a loaf of bread every week, but it would be odd to say that I am “manufacturing” bookshelves or shirts or bread. In addition, it is clear from the legislative history that the device bans in § 1201 were designed to prevent large-scale circumvention and to penalize those who would assist others in circumventing activities. As Register Peters stated:

Because of the difficulty involved in discovering and obtaining meaningful relief from individuals who engage in acts of circumvention, a broader prohibition extending to those *in the business* of providing the means for circumvention appears to be necessary to make the protection adequate and effective [as required by treaty]. It is the conduct of *commercial suppliers* that will enable and result in large-scale circumvention.

Statement of Marybeth Peters, *supra* note 71, at 48 (emphasis added); *see also* Samuelson, *supra* note 2, at 555 (noting that proponents testified before Congress that anti-device provisions were “needed to stop deliberate and systematic piracy by ‘black box’ providers”). Thus, someone who produces a single circumvention device for her own use might well not be violating the device bans, and if she used the device to circumvent a rights control and make a noninfringing use of the protected work, she would face no legal liability whatsoever. That result seems entirely in line with the express congressional intent of preserving consumers' ability to make noninfringing uses.

122. As discussed in Part II.A.2 above, devices that circumvent a technological measure that both protects a right of the copyright owner and prevents noninfringing uses might not be an illegal circumvention device.

123. *See supra* notes 15-17 and accompanying text.

copy because copyright law allows her use of the work.¹²⁴ But if the rights-control measure was part of a merged access and rights control, she might face liability for violating § 1201(a)(1) because she has probably circumvented the access control as well as the rights control. In this instance, enforcing the act ban is inconsistent with the statute's refusal to impose liability on the copier for circumventing a rights control in order to engage in noninfringing activity. Thus, if Congress was serious about exempting acts circumventing rights controls from liability in order to allow noninfringing uses, merged control measures will require statutory adjustments.

B. Permit Acts Circumventing Access Controls *If Purpose Is to Engage in Noninfringing Use*

Congress apparently thought that by not restricting acts circumventing rights-control measures, noninfringing uses of copyrighted works would continue even as copyright owners deploy legally protected technological protection measures. However, protecting merged control measures as both access and rights controls may thwart this plan. To effectuate the congressional intent to allow noninfringing circumvention, an exemption from § 1201(a)(1)'s ban on circumventing acts might be needed.

The simplest way to allow circumvention of merged control measures for noninfringing purposes is to tie liability under § 1201(a)(1) in such situations to copyright infringement. If someone circumventing a merged access and rights control would not be liable for copyright infringement, then she would also not be liable under § 1201(a)(1) for circumventing the access control, just as she would not be liable under § 1201(b) for circumventing the rights control. Congress could add such an exemption to § 1201.

Not only does such an exemption protect the breathing space that Congress allowed for noninfringing circumvention, it also would not necessarily have a significant undue impact on Chapter 12's overall level of legal protection for copyright owners' use of technological protection measures. This exemption would not apply to the device ban of § 1201(a)(2).¹²⁵ As a result, those wanting to circumvent merged control

124. See *supra* notes 15-17 and accompanying text.

125. This is not to suggest that the device bans in Chapter 12 are not themselves problematic. As many commentators have noted, the breadth of those bans may mean that very few people—the highly technologically skilled—will in practice be able to engage in the specifically permitted acts of circumvention, since the vast majority of those who might want to engage in such circumvention will not be able to do so without acquiring technology from someone else. See, e.g., Band & Issihiki, *supra* note 67, at 6 (noting that exception allowing circumvention to protect personally identifying information does

ANTICIRCUMVENTION LAW

measures for noninfringing purposes would have to either be sufficiently technologically savvy to create their own device or acquire a circumventing device. If such a device may be legally manufactured and distributed under § 1201(a)(2), then not penalizing those who use the device for noninfringing purposes is unlikely to seriously undermine § 1201(a)(1)'s protection of the copyright owner. Indeed, as a practical matter, detection of dispersed, private circumventing uses of the device—whether those uses are legal or illegal—will likely remain difficult. By contrast, if the device violates § 1201(a)(2), then those who manufacture or traffic in the device would be subject to liability. Exempting from liability those users who use the illegal device for noninfringing purposes is unlikely to significantly hamper enforcement against device manufacturers and traffickers. Congress included the anti-device provisions, after all, because enforcement against individual users was perceived as more difficult than against those supplying circumvention technologies.

The fact that some additional acts of circumvention—circumvention of merged control measures for noninfringing purposes—would be allowed under § 1201(a)(1) also does not necessarily affect the circumvention device ban under § 1201(a)(2). Devices are prohibited if they are “primarily designed or produced for the purpose of circumventing” an access-control measure or if they have “only limited commercially significant purpose or use other than” such circumvention.¹²⁶ If noninfringing circumvention of merged control measures is allowed, a greater number of uses of a circumvention device may be permitted. Those uses, however, would still be circumventing uses. The device bans do not bar technologies that have limited commercially significant purpose or use other than engaging in *prohibited* circumvention of an access control. The statutory language suggests that even permitted circumvention will not count in favor of a device in determining the device's primary purpose or commercially significant uses. The key issue under the statute is whether the purpose and use of the technology is to circumvent an access-control measure, not

not apply to device bans and therefore “[i]t is not clear how users are expected to effectuate [permitted] circumvention if developers are not permitted to manufacture and distribute circumvention devices”); Burk & Cohen, *supra* note 32, at 49-50 (“As a practical matter . . . any exemptions ultimately declared [by the Librarian of Congress] will have very limited utility; self-evidently, most users will be unable to exercise their circumvention rights unless they are provided with the tools to do so.”); Samuelson, *supra* note 2, at 551. Any more general reworking of the device bans should, of course, take into account the problem of merged controls, but the problems of the device bans generally are beyond the scope of this Article.

126. 17 U.S.C. § 1201(a)(2)(A)-(B) (2000).

whether such circumvention is allowed.¹²⁷ A device that has a commercially significant purpose of making statutorily permitted circumvention of an access-control measure (such as circumvention to protect personally identifying information¹²⁸) is still a device without a commercially significant purpose other than circumventing an access control, and thus likely prohibited under § 1201(a)(2).¹²⁹

A final concern raised by such an exemption might be that some circumvention, even of merged control measures, should remain prohibited. While merged controls may be aimed largely at limiting copying or dissemination of the protected work, as in *RealNetworks* and *Reimerdes*, they might actually be intended to control access to copyrighted works independently of their control on copying. For example, a trusted system might allow a user to purchase a digital copy of a motion picture for two different prices, one price for a copy without any restrictions on use (other than those imposed by copyright law) and a lower price for a copy that may be played only for a twenty-four-hour period during the first thirty days after the copy is purchased. This would be a quintessential access control system. As Jane Ginsburg has explained, “In theory, access controls are designed to protect a business model based on price discrimination according to intensity of use.”¹³⁰ If a merged control measure is in fact aimed substantially at controlling access, then an exemption allowing a user to circumvent a merged control whenever the user’s post-circumvention use is noninfringing may be too broad. For instance, someone who buys a time-limited copy of a copyrighted work and then circumvents the access control in order to view the work privately after the time limit has expired would probably be covered by the exemption, since the post-

127. Indeed, there might otherwise be little need for the specific exemptions from the device bans in § 1201(a) and § 1201(b), since devices needed for exempted acts of circumvention for purposes of reverse engineering, security testing, and encryption research would have purposes other than *prohibited* circumvention: they could be used for *permitted* circumvention.

128. 17 U.S.C. § 1201(i).

129. Because of the language of the device bans, though, a device’s usefulness for circumventing protection measures applied to works not protected by copyright law is relevant in determining whether the device is prohibited. *Id.* § 1201(a)(2), (b)(1) (defining prohibited technology by its uses for circumventing technology that “controls access to a work protected under this title” or that “protects a right of a copyright owner under this title in a work”). Thus, if a device has a commercially significant purpose of circumventing access measures that control access to works in the public domain, it would not be illegal under 17 U.S.C. § 1201(a)(2)(B). Its legality would still, however, depend on the purpose for which it was “primarily designed or produced,” and on the way in which it is marketed. *Id.* § 1201(a)(2)(A), (C).

130. Ginsburg, *supra* note 26, at 16.

ANTICIRCUMVENTION LAW

circumvention private performance of the work would not be a copyright infringement. It is unclear, however, that circumvention of the merged control measure for this purpose should be allowed.

Thus, an exemption allowing noninfringing circumvention of merged controls might cut more broadly than necessary to avoid interference with the congressional goal of allowing circumvention of rights controls for noninfringing purposes. This potential overbreadth might, however, simply be accepted. After all, the permitted activity is likely to be small in quantity, since only technologically skilled persons would be able to commit such circumventing acts. Moreover, such acts are unlikely actually to be penalized even under the current statute without a merged-control exemption, since such circumvention occurs in private. If, on the other hand, the permitted undesirable activity is significant enough to warrant imposing § 1201(a)(1)'s prohibition, the exemption could be more narrowly drawn. It might distinguish between different types of merged control measures, allowing noninfringing circumvention where the control is primarily operating as a rights control but not where it primarily operates as an access control. Or it might distinguish between types of circumventions, exempting only those designed to do something more than merely obtain unauthorized access to a work without payment.¹³¹

The forum in which the exemption is adopted could determine the precise scope of an exemption from the circumvention ban in the case of merged control measures. The most obvious forum is Congress, which could amend the statute to provide for the exemption. Another possible forum is a Copyright Office rulemaking. Section 1201(a)(1) directs the Librarian of Congress to hold a rulemaking proceeding every three years to determine whether the ban on access-control circumvention is likely to adversely affect users' ability to make noninfringing uses of any "particular class of copyrighted works."¹³² If the Librarian makes such a determination, then the circumvention ban does not apply to users of a copyrighted work that is in the identified "particular class."¹³³ The statute thus

131. Commentators have suggested this type of approach for other applications of § 1201(a). *See, e.g.*, Ginsburg, *supra* note 26, at 16 ("[I]t may become necessary to modify the scope of the § 1201(a) access right, to continue to provide strong protection against unauthorized *initial* acquisition of a copy of a protected work, but to allow for circumvention in order to engage in fair uses, once the copy has been lawfully acquired."); Samuelson, *supra* note 2, at 539 ("Courts should distinguish between circumvention aimed at getting unauthorized access to a work and circumvention aimed at making noninfringing uses of a lawfully obtained copy. Section 1201(a)(1) is aimed at the former, not the latter.") (citations omitted).

132. 17 U.S.C. § 1201(a)(1)(C).

133. *Id.* § 1201(a)(1)(B), (D).

gives the Librarian, on recommendation of the Register of Copyrights, the power to adopt temporary, partial exemptions to the circumvention ban (though not to either of the device bans).

The Librarian's first rulemaking proceeding under the statute was completed in October 2000, and briefly considered the possibility of an exemption with respect to merged control measures. The Register, however, concluded that, at the time of the rulemaking, the evidence did not establish that merged control measures posed a significant enough problem to require that the rulemaking address it.¹³⁴ Nonetheless, the Register noted that "[i]f in a subsequent rulemaking proceeding one could show that a particular 'copy' or 'use' control could not in fact be circumvented on a legitimately acquired copy without also circumventing the access measure, one might meet the required burden on this issue [of substantial or concrete harm to users]."¹³⁵ The Copyright Office stated its intent to continue to monitor the issue and perhaps to consider it in connection with future exemption rulemakings.¹³⁶

At least two features of the rulemaking proceeding, however, suggest that it is not a hospitable forum for providing relief to those who wish to circumvent a merged control measure in order to engage in noninfringing use. The first problem is that the statute empowers the Librarian to adopt an exemption from the circumvention ban if users are likely to be adversely affected in their ability to make noninfringing uses of any "particular class of works."¹³⁷ In the 2000 rulemaking, the Register, however, rejected any definition of a class of works "based on the status of the user or the nature of the use."¹³⁸ This may make it difficult to adopt an appropriate exemption for merged control measures. As discussed above, an appropriately tailored limitation on § 1201(a)(1) for merged controls would exempt from liability anyone who circumvents a merged control to make a

134. Exemption to Prohibition on Circumvention of Copyright Protection Systems for Access Control Technologies, 65 Fed. Reg. 64,556, 64,568 (Oct. 27, 2000).

135. *Id.*

136. *See id.* The Copyright Office specifically stated:

At present, on the current record, it would be imprudent to venture too far on this issue in the absence of congressional guidance. The issue of merged access and use measures may become a significant problem. The Copyright Office intends to monitor this issue during the next three years and hopes to have the benefit of a clearer record and guidance from Congress at the time of the next rulemaking proceeding.

Id.

137. 17 U.S.C. § 1201(a)(1)(B)-(D).

138. Exemption to Prohibition on Circumvention of Copyright Protection Systems for Access Control Technologies, 65 Fed. Reg. at 64,560.

ANTICIRCUMVENTION LAW

noninfringing use of the work protected by the control. That exemption, however, would require defining the “particular class of works” to which the exemption applies by reference in part to the nature of the use to be made by the circumventing party—a definitional criterion expressly rejected by the Register of Copyrights in 2000 as beyond the statutory scope of the Librarian of Congress’s rulemaking authority.¹³⁹

A second difficulty in solving the merged control problem through the triennial rulemaking is the high burden that proponents of an exemption must meet in order to persuade the Librarian to act. The 2000 rulemaking made clear that those proposing an exemption bear the burden of demonstrating that § 1201(a)(1)’s ban on circumvention “has a substantial adverse effect on noninfringing use,” and that the decisionmaker will focus on whether there are “distinct, verifiable, and measurable impacts.”¹⁴⁰ This standard could be difficult to meet with respect to the impact of merged control measures on noninfringing users. The Copyright Office has indicated that if an access control’s adverse effect on noninfringing uses is “confined to a relatively small number of users,” then the adverse effect does not rise to the “substantial” level required to adopt an exemption.¹⁴¹ Because most circumvention devices seem likely to be prohibited even where people could use those devices to circumvent access or rights controls in order to make noninfringing uses, those adversely affected by treating a merged control measure as an access control are those who wish to circumvent the merged control in order to make noninfringing uses *and* who have the technological capability to do so.¹⁴² That seems likely, in most cases, to be a relatively small number of people. The rulemaking proceeding may therefore view the adverse affect of protecting merged

139. The Register did recognize the permissibility for rulemaking purposes of classifying works *in part* “by reference to the medium on which the works are distributed or even to the access control measures applied to them.” *Id.* Thus, for example, an exemption might be possible for musical works and sound recordings distributed on CD using a specific merged control system. But such an exemption would still be too broad, since it would exempt from liability for circumvention both those who, post-circumvention, engage in permitted uses and those who engage in outright infringement.

140. *Id.* at 64,558.

141. *Id.* at 64,569.

142. While the number of people directly adversely affected may be small, they may be a particularly important group for copyright purposes. Particularly where the person wishing to circumvent a merged control wants to do so in order to make a transformative fair use of the work, the benefit of the post-circumvention use may extend far beyond the user, to all of those who might encounter the transformative work. After all, creators and publishers of works of authorship may be a relatively small group of people as part of the nation’s entire population, but we consider them particularly deserving of protection for their work because the rest of the population benefits substantially from their efforts.

control measures as access controls as *de minimis* and not within the Librarian's power to address.

These problems suggest that the triennial rulemaking under § 1201(a)(1) may not be well suited to address concerns about the effect of merged control measures on noninfringing uses of copyrighted works. Indeed, the Register herself noted the rather constrained scope of the Librarian's rulemaking authority in the first rulemaking proceeding: "While many commenters and witnesses made eloquent policy arguments in support of exemptions for certain types of works or certain uses of works, such arguments in most cases are more appropriately directed to the legislator rather than the regulator who is operating under the constraints imposed by section 1201(a)(1)."¹⁴³ The need to address the problems posed by merged control measures may similarly be a concern better directed to Congress than to the Librarian.

C. Exempt Noninfringing Circumvention of Merged Control Measures as Part of Broader Limitation on Rights Against Circumvention

Another way to ensure that those who wish to circumvent a merged control measure for noninfringing purposes may do so would be to adopt more general limitations on the ban against circumventing access-control measures. As Jane Ginsburg has noted, copyright law traditionally did not grant copyright owners an exclusive right of access to their works once they are made publicly available, but § 1201 may effectively grant such a right. Professor Ginsburg further points out that because Chapter 12 does not protect an author's control over access as a § 106 exclusive right under copyright law, the copyright owner's control over access is not subject to the normal limitations imposed on copyright rights, including fair use. Instead, the copyright owner's control over access is subject only to the very limited exceptions listed in § 1201.¹⁴⁴ This clearly presents difficulties for copyright law's traditional role of balancing the interests of copyright owners and the public:

[W]ithout an appropriate fair use limitation, the access right under § 1201 becomes much more than such a component [of copyright]. It becomes instead an Uber-copyright law, rigid as to

143. Exemption to Prohibition on Circumvention of Copyright Protection Systems for Access Control Technologies, 65 Fed. Reg. at 64,562.

144. See Ginsburg, *supra* note 26, at 11 ("[A]ccess controls may be a measure too crude to accommodate a variety of non infringing uses, including reproduction of unprotected information contained within a copyrighted work, and 'transformative' fair uses . . .").

ANTICIRCUMVENTION LAW

specified exceptions, and therefore freed of further inquiry into the balance of copyright owner rights and user privileges that the fair use doctrine—and the general structure of copyright law—require.¹⁴⁵

Professor Ginsburg therefore recommends subjecting copyright owners' legal right to prevent circumvention of access controls under § 1201 to additional exemptions that take into account the copyright system's need to allow unauthorized access and use of copyrighted works in some instances.¹⁴⁶

Indeed, Professor Ginsburg suggests that it might be necessary to modify § 1201 “to allow for circumvention in order to engage in fair uses,” once a user has lawfully acquired a copy of the protected work.¹⁴⁷ The statute might, for example, provide that the act of circumvention is fair if a circumventor's post-circumvention use qualifies as fair use. Or the statute might direct a court in such an instance to weigh all of the circumstances surrounding the circumvention to determine whether to allow the circumvention, just as courts in copyright infringement cases weigh all of the circumstances surrounding a defendant's use of copyrighted material in order to determine whether the use is a fair use.

Such a general approach to limiting the copyright owner's legal control over access via technological protections could also easily accommodate the specific concerns relating to merged control measures.¹⁴⁸ Someone who circumvents a merged control measure in order to make a noninfringing use of the protected work engages in conduct that copyright law has chosen to privilege by excluding it from the copyright owner's exclusive rights. A general exemption from the ban on circumventing access controls where the circumvention merely allows the user to make entirely legal uses of the work would address the principal difficulty raised by copyright owners' use of merged control measures. Two current legisla-

145. *Id.* at 17.

146. *Id.* at 16 (noting that “some traditional defenses may remain appropriate, others may not, but new ones may be needed”); *see also* Thomas Heide, *Copyright in the E.U. and United States: What “Access Right”?*, 2001 EUR. INTELL. PROP. REV. 469, 475-77 (“From this perspective, it becomes necessary to apply appropriate safeguard measures so that rights and limitations to copyright remain unaffected and introduce appropriate limitations and exceptions to any access centered rights structure.”).

147. Ginsburg, *supra* note 26, at 16.

148. On the other hand, if the kinds of limitations on access controls that Professor Ginsburg proposes were to be adopted by means of a set of more specific exemptions, then one of those exemptions could address the specific problem of merged controls.

tive proposals would provide such a general exemption.¹⁴⁹ Both would allow the circumvention of access and rights controls if the circumventing party did not commit copyright infringement.

V. CONCLUSION

Copyright owners who wish to use technological measures to protect their works no doubt consider many variables in choosing which controls to use. Many of those variables may have little or nothing to do with the law, but the nature and degree of legal protection available against circumvention of technological controls no doubt plays at least a part in the decision for many copyright owners. Copyright owners seeking the maximum legal protection possible for their control systems may adopt systems that merge an access-control mechanism and a rights-control mechanism into a single system because of the added protection such a choice would provide. But if such merged control measures enjoy all the protection of both access controls and rights controls, then Congress's objective in carefully treating the different types of control measures distinctly in order to provide breathing room for noninfringing uses of copyrighted works will be significantly undermined. Congress should therefore consider amending the anticircumvention provisions of the Copyright Act to deal specifically with merged control measures in a way that continues to protect copyright owners' rights and the public's ability to make noninfringing uses.

149. *See* Digital Media Consumers' Rights Act of 2003, H.R. 107, 108th Cong. (2003); Digital Choice and Freedom Act of 2003, H.R. 1066, 108th Cong. (2003). The former bill would allow circumvention if it "does not result in an infringement of the copyright in the [protected] work," H.R. 107 § 5(b), while the latter would permit circumvention if "necessary to make a non-infringing use of the [protected] work" and if "the copyright owner fails to make publicly available the necessary means to make such non-infringing use without additional cost or burden" to the user, H.R. 1066 § 5. In addition, both bills would allow the manufacture and dissemination of circumvention devices for noninfringing purposes. *See* H.R. 107 § 5(b); H.R. 1066 § 5.

ANTIRCUMVENTION LAW