Harvard Journal of Law & Technology
Volume 20, Number 1 Fall 2006

DIGITAL RIGHTS MANAGEMENT AND THE PROCESS OF FAIR USE

*Timothy K. Armstrong**

TABLE OF CONTENTS

---

* Assistant Professor of Law, University of Cincinnati College of Law. B.A. 1989, M.P.Aff. 1993, J.D. 1993, The University of Texas at Austin; LL.M. 2005, Harvard Law School. I am grateful for the advice and input of many of my colleagues at the Berkman Center for Internet & Society at Harvard Law School. Jonathan Zittrain reviewed and commented on a much lengthier version of the manuscript that became this article. John Palfrey, Urs Gasser, and the members of the Berkman Center's Digital Media Project first pointed me towards research on technological accommodations for fair use. Derek Bambauer and Stefan Bechtold closely reviewed the manuscript and offered detailed critiques. The remaining flaws of this paper flow largely from my incomplete adherence to their suggestions, for which of course I have only myself to blame.

I. INTRODUCTION: LEGAL AND TECHNOLOGICAL PROTECTIONS FOR FAIR USE OF COPYRIGHTED WORKS

United States copyright law nominally grants consumers the right to make "fair use" of copyrighted works.[1] When the copyrighted work is distributed in digital form, however, technological impediments may, as a practical matter, prevent some uses of the work that the law would recognize as fair. Distributors of copyrighted digital works may deploy "digital rights management" ("DRM") mechanisms that allow only certain types of access to, or uses of, the underlying copyrighted work and forbid all others.[2] Although technologically sophisticated users may be able to bypass a DRM mechanism and obtain greater

1. Although I will follow common usage herein in speaking of fair use as a "right," it is, more precisely, a statutory immunity from liability for acts that would otherwise amount to copyright infringement. For a conception that places users' rights at the center, rather than the periphery, of fair use analysis, see L. RAY PATTERSON & STANLEY W. LINDBERG, THE NATURE OF COPYRIGHT: A LAW OF USERS' RIGHTS ch. 14 (1991). *See also id.* at 103–06 (arguing that the wording of the fair use statute perversely works to enhance copyright holders' monopoly insofar as it is vague and drafted from the copyright holder's vantage point). The fair use doctrine is presently codified in 17 U.S.C. § 107 (2000).

2. An accessible overview of DRM technology is available in GARTNERG2 & THE BERKMAN CENTER FOR INTERNET & SOCIETY AT HARVARD LAW SCHOOL, COPYRIGHT AND DIGITAL MEDIA IN A POST-NAPSTER WORLD 43–50 (2d ed. 2005), http://cyber.law.harvard.edu/media/files/wp2005.pdf. The umbrella term "DRM" describes a class of technologies, the particulars of which vary from one implementation to the next. The details of a few particular implementations will be taken up below. *See infra* notes 59–65 and accompanying text (describing DRM mechanisms employed to protect digital music downloads and DVD video discs).

access to the work than the DRM mechanism is intended to permit,[3] such circumvention may violate the Digital Millennium Copyright Act of 1998 ("DMCA").[4] DRM technology and the DMCA have been controversial in academic and technological circles: copyright holders may deploy DRM mechanisms that do not allow fair uses of the copyrighted work and the DMCA may protect such mechanisms against circumvention, resulting in a curtailment of consumers' ability to engage in lawful fair uses of digital copyrighted works.[5]

As more and more copyrighted content is released in digital form, the risk of a shrinking domain for fair use has inspired some observers to ask whether DRM technology may evolve to preserve end user freedoms. On this view, DRM technology need not be inherently restrictive of fair use rights. Rather, limiting fair use via DRM is simply one choice among many alternative design decisions that DRM architects might adopt.[6] Protecting fair use of digital content would simply involve tweaking, rather than circumventing, the DRM mechanisms employed to protect the underlying copyrighted work. By fostering instead of preventing fair use, future DRM technologies might reduce the present disunion between what the law permits and what technology enables.[7]

---

3. *See Competition, Innovation, and Public Policy in the Digital Age: Is the Marketplace Working to Protect Digital Creative Works Before the S. Comm. on the Judiciary*, 107th Cong. 2 (2002) [hereinafter *Felten Testimony*] (statement of Edward W. Felten, Associate Professor of Computer Science, Princeton University) ("[S]trong copy protection (protection that a moderately skilled person expending moderate effort cannot break) simply is not possible on general purpose computers . . . [and] is as implausible to many experts as a perpetual motion machine."), *available at* http://www.freedom-to-tinker.com/felten_testimony.pdf.

4. Pub. L. No. 105-304, 112 Stat. 2360 (1998) (codified as amended at 17 U.S.C. §§ 1201–1205). For a summary of the key events leading to the passage of the DMCA, see WILLIAM W. FISHER III, PROMISES TO KEEP: TECHNOLOGY, LAW, AND THE FUTURE OF ENTERTAINMENT 90–93 (2004); JESSICA LITMAN, DIGITAL COPYRIGHT 122–45 (2001). *See generally infra* Part II.B.2.

5. *See, e.g.*, David Nimmer, *A Riff on Fair Use in the Digital Millennium Copyright Act*, 148 U. PA. L. REV. 673, 739–40 (2000); Matt Jackson, *Using Technology to Circumvent the Law: The DMCA's Push to Privatize Copyright*, 23 HASTINGS COMM. & ENT. L.J. 607, 638 (2001) (arguing that the DMCA "threatens precisely these legitimate [fair] uses of copyrighted texts"); ELECTRONIC FRONTIER FOUNDATION, UNINTENDED CONSEQUENCES: FIVE YEARS UNDER THE DMCA 7–9 (2003), http://www.eff.org/IP/DMCA/unintended_consequences.pdf.

6. *See* Stefan Bechtold, *The Present and Future of Digital Rights Management — Musings on Emerging Legal Problems*, *in* DIGITAL RIGHTS MANAGEMENT — TECHNOLOGICAL, ECONOMIC, LEGAL AND POLITICAL ASPECTS, LNCS 2770, at 597, 603 (Eberhard Becker et al. eds., 2003) (noting that nothing inherent in DRM technology makes it impossible to design DRM systems that are more accommodating of end user rights than most contemporary DRM implementations).

7. On the range of choices available to future designers of DRM technologies, see, for example, Stefan Bechtold, *Value-Centered Design of Digital Rights Management: Perspectives on an Emerging Scholarship*, INDICARE MONITOR, Sept. 9, 2004, http://www.indicare.org/tiki-read_article.php?articleId=39.

The conventional wisdom is justifiably skeptical of the notion that copyright's fair use doctrine, which legally depends upon balancing a number of highly malleable contextual factors,[8] might ever be reduced to something that can be administered by machine. The balancing test established in the fair use statute does not specify the substance of the factors that must be considered or the relative weights that should be given to each, and the very nature of some of the factors is such that they cannot readily be reduced to binary logic. For these reasons, some computer scientists argue that a computer cannot be programmed to accurately reproduce the decisions that a human judge would render in an individual case, and therefore cannot effectively substitute for human decisionmaking in administering the fair use doctrine.[9] A recent government report summarizes the conventional view:

> The copyright law, although carefully worded, simply cannot be expressed in the kind of algorithmic language that is required by computer programs to automate functionality like printing or copying. This is especially true of the key concept of "fair use." Fair use is a deliberately vague exception to the monopoly rights of the copyright holder. It says essentially that although the copyright holder has the exclusive right to make copies of the work, members of the public can also make copies if their use is "fair." There is no *a priori* test for whether a use is fair; each such exercise of the public's right must be carefully scrutinized taking into account a number of factors. Even after such scrutiny, not everyone will agree on what is fair. Electronic systems need an unambiguous and quantitative definition that they can act on, and the copyright law does not provide that.[10]

Other recent scholarship, however, suggests that this received orthodoxy may be ripe for re-examination. Efforts to provide technological protection for fair use rights have evolved in unexpected

---

8. *See infra* notes 30–31.

9. *See* Edward W. Felten, *A Skeptical View of DRM and Fair Use*, COMM. ACM, Apr. 2003, at 56.

10. KAREN COYLE, RIGHTS EXPRESSION LANGUAGES: A REPORT FOR THE LIBRARY OF CONGRESS 11 (Feb. 2004), http://www.loc.gov/standards/Coylereport_final1single.pdf; s*ee also* WILLIAM ROSENBLATT ET AL., DIGITAL RIGHTS MANAGEMENT: BUSINESS AND TECHNOLOGY 45 (2002); David Nimmer, *"Fairest of Them All" and Other Fairy Tales of Fair Use*, 66 LAW & CONTEMP. PROBS. 263, 284 (2003) ("[I]t seems unlikely that anyone will develop a heuristic device for computer programs to calculate when fair use should apply — at least, any time before machines become human."); *infra* notes 101–05.

directions,[11] and legal scholars have pushed to identify with particularity what practical hurdles must be overcome for fair use to receive technological protection.[12]

The driving insight of these new approaches is a de-emphasis on the substance of copyright law and a new stress on process. We cannot have a "judge on a chip" — an electronic system that balances the statutory factors (and whatever nonstatutory factors a human judge would consider) and unerringly produces the same decision that a human judge would render in any individual case. But is such a "judge on a chip" indispensable to protecting fair use of digital content? Outside the digital arena, fair uses of copyrighted works are not subject to DRM-like prior review, permission, or restraint by copyright holders or their designees. Taking user experiences with copyrighted works in the offline world as our baseline, we might set the goal of creating similar opportunities for fair use of digital works.[13] As one observer put it, when it comes to designing technological protections for fair use, it is

> clear that many DRM vendors are asking precisely the wrong question. The approach should not be "tell me what fair use requires, and I'll build it in" but rather "how can I build something that permits a variety of as-yet unknown uses, so that courts can decide whether those future uses are fair."[14]

Creating systems that unlock the *process* of fair use, while still providing copyright owners with technological protections against infringement, is a challenge that requires neither creating a "judge on a chip" nor jettisoning the legitimate protections that DRM measures provide.

Authors have offered a variety of proposals aimed at incorporating protections for fair use into DRM technologies. These have ranged from the simplistic (hard-coding an agreed subset of clearly fair uses into a user's copy of DRM-protected content)[15] to the highly sophisticated (combining preauthorized fair use defaults with an interactive remote authorization mechanism to acquire additional permissions).[16] At bottom, however, virtually all these proposals suffer from a com-

---

11. *See infra* Part IV.A.3.

12. *See infra* Part IV.A.2.

13. Throughout this Article, I will use the term the "offline world" to refer to copyrighted works that are not protected by DRM, even though DRM protections can be used in digital works that do not appear on the Internet or any network. This term merely seeks to contrast past conventional fair use experiences with experiences using works protected by DRM.

14. FRED VON LOHMANN, RECONCILING DRM AND FAIR USE: PRESERVING FUTURE FAIR USES? 1 (2002), http://www.cfp2002.org/fairuse/lohmann.pdf.

15. *See infra* notes 95–97 and accompanying text.

16. *See infra* notes 142–52 and accompanying text.

mon flaw: although they may employ very sophisticated authorization models that permit a variety of interactions and responses between users and content providers, each of the proposals creates a burden of obtaining consent that has no parallel in the offline world. Stated slightly differently, every permissions-based DRM implementation (in which the user must formally acquire some form of explicit authorization to engage in a particular use of the protected work) simply reproduces a variant of the "judge on a chip" problem. No such system can ever replicate the experience of fair use in the offline world because the requirement of *ex ante* authorization by the copyright holder or its designee is a departure from offline practice and statutory requirements.[17]

Recent academic work suggests a new direction for protecting fair use in the digital arena. Authors looking at the issue from both legal and technological standpoints have begun to outline a new framework that would allow end users greater latitude to make fair uses of digital content. For example, future DRM implementations might include a new messaging layer that would allow authorizations to be communicated from multiple sources, potentially even from users themselves.[18] One such proposed DRM system, aimed expressly at preserving end users' fair use rights, has been developed by a team of academic and industry computer scientists from the Netherlands. Their proposal expands upon traditional DRM systems by allowing end users to assert new rights not previously granted by the content provider, while protecting the copyright holder against abuse by logging each such assertion for subsequent review.[19]

The remainder of this Article explores the development of DRM technologies aimed at preserving practical opportunities for fair use of digital content. Part II begins with an examination of copyright law, the historical uses of DRM technologies, and accompanying statutory protections against circumvention of DRM. The historical overview is intended to establish a policy baseline for evaluating existing and proposed protections for fair use in the context of digital media. I contend that a system of digital media regulation that accepts, as a baseline, the reasonable expectations of fair use that users have derived over a lifetime of interactions with ordinary offline media is preferable to a system that frustrates these expectations.[20] One's inclination to accept,

17. *See infra* note 178 and accompanying text.

18. *See infra* Parts IV.A.1, IV.A.2.

19. *See infra* Part IV.A.3.

20. This approach is admittedly conservative. The ever-expanding pool of media content available in digital form, coupled with the widespread availability of sophisticated authoring tools even on entry-level computer hardware, collectively blurs distinctions between producers and consumers and invites the formulation of new approaches to fair use that better capture the many types of creative interactions users may experience with digital media. *See, e.g.*, Yochai Benkler, *From Consumers to Users: Shifting the Deeper Structures of Regulation Toward Sustainable Commons and User Access*, 52 FED. COMM. L.J. 561

or to dispute, my position should prove a reliable guide to the reader's receptiveness to the remainder of my argument.[21]

Part III continues with a comparative assessment of a variety of existing and proposed DRM systems, describing how each system provides, or fails to provide, robust protections for fair use. I will develop two critical observations in this portion of the Article. First, the efficacy of any DRM system for protecting fair use depends in large measure on the extent to which the system grants parties other than the copyright holder — such as the government, a third party licensing authority, or the end user — a say in whether any individual use, or category of uses, will be permitted. Existing DRM technologies offer poor protections for fair use because the determination of which uses are permitted is largely at the discretion of copyright holders or their designees. Second, protections for fair use in any DRM system are partly a function of the particular language the designers of that system employ to express digital rights information. Although the most widespread DRM implementations available today adopt a "closed-universe" approach in which any right not described by the system is deemed not to exist, proposed alternative systems would establish different default behaviors that may better accommodate fair use rights.

Part IV examines recent DRM proposals that would incorporate varying levels of input from end users into the process of unlocking and accessing the underlying copyrighted works and describes a system that would provide protections for consumers of digital content comparable to those in the offline arena. The emphasis here is on solving the "judge on a chip" problem by allowing the scope of machine-recognized user "permissions" to expand dynamically in re-

---

(2000). The literature has already begun to grapple with the implications for DRM design of a universe in which all consumers are simultaneously potential creators whose rights in their own creations must receive protection comparable to other copyright holders' rights. *See, e.g.*, Akiko Seki & Wataru Kameyama, *A Proposal on Open DRM System Coping with Both Benefits of Rights-Holders and Users*, *in* IEEE GLOBAL TELECOMMUNICATIONS CONFERENCE: COMMUNICATIONS, GLOBECOM 2003, at 4111 (2003); *infra* note 126.

My aim here is not to freeze the legal or policy analysis of fair use to what exists presently in the offline world, but rather to use the offline policy baseline to illuminate the ways that DRM currently protects (or fails to protect) fair use. Indeed, the ultimate benefit of a DRM system engineered to protect fair use as a process, rather than attempting to hard-code the substantive law of fair use, would be the liberation of fair use doctrine so that it can continue to evolve on a case-by-case basis in response to users' actions.

Although I have spoken of the beneficiaries of the fair use doctrine as both "consumers" and "users," I will use the latter formulation in the remainder of this Article — an etymological choice that on the one hand adheres to convention, but on the other carries unavoidable normative significance. *See* Julie E. Cohen, *The Place of the User in Copyright Law*, 74 FORDHAM L. REV. 347 (2005).

21. For a contrary view that DRM restrictions imposed by the copyright holder not only *can*, but *should*, trump individual expectations regarding fair use in the digital domain, see Ben Fernandez, Note, *Content Protection and Fair Use: What's the Use?*, 3 J. ON TELECOMM. & HIGH TECH. L. 425 (2005).

sponse to a user's assertion of fair use rights without *ex ante* involvement of the copyright holder. The three most prominent components of the system developed in this part of the article, all of which are drawn from prior technical literature on DRM, are (1) a *user rights assertion* framework whereby users may acquire the power to access or use the protected work in any fashion they wish without the necessity of prior approval by an outside decisionmaker; (2) an *audit logging* mechanism that preserves information about such rights assertions; and (3) an *identity escrow* framework employing cryptographic techniques to shield the identity of users (except upon a proper showing of cause). Part V considers a number of legal and political issues connected with the implementation of fair use protections in DRM mechanisms. Finally, Part VI concludes that DRM mechanisms engineered to protect fair use rights are in the long-term interests of both content providers and consumers.[22]

II. COPYRIGHT LAW AND/OR DIGITAL RIGHTS MANAGEMENT[23]

A. Traditional Copyright: The Normative Baseline

From the moment a creative work[24] is fixed in a tangible medium of expression,[25] the creator of the work enjoys statutorily enumerated exclusive rights, including the rights to make and distribute copies of the work, to perform the work publicly, and to prepare derivative works.[26] Because the copyright statute aims to protect users as well as copyright holders,[27] the copyright holder enjoys its exclusive rights

22. In these sections, and throughout this article, I will assume that the fair use issue remains relevant in any particular case — that is to say, that the user of DRM-protected content actually enjoys the right to engage in fair uses of the underlying work and has not, for example, voluntarily relinquished that right by contract. *Cf.* Dennis S. Karjala, *Federal Preemption of Shrinkwrap and On-Line Licenses*, 22 U. DAYTON L. REV. 511, 525–33 (1997) (arguing that non-negotiated waiver of fair use rights, such as under a shrinkwrap license, should be deemed preempted by the Copyright Act); Lydia Pallas Loren, *Slaying the Leather-Winged Demons in the Night: Reforming Copyright Owner Contracting with Clickwrap Misuse*, 30 OHIO N.U. L. REV. 495, 512–35 (2004) (arguing that contractual clauses requiring waiver of end user copyright rights should be presumed invalid on grounds of copyright misuse, although the presumption could be rebutted by the copyright holder).

23. For the inspiration behind the title of this Part, see Pamela Samuelson, *DRM {and, or, vs.} the Law*, COMM. ACM, Apr. 2003, at 41.

24. *See* Feist Publ'ns, Inc. v. Rural Tel. Serv. Co., 499 U.S. 340, 345 (1991) (explaining that "at least some minimal degree of creativity" is a prerequisite to copyrightability).

25. 17 U.S.C. § 102(a) (2000).

26. *Id.* § 106.

27. The notion of a balance between the interests of copyright holders on the one hand, and users of creative works on the other, recurs frequently in copyright discourse. The Supreme Court has consistently described copyright not only as a monopoly grant to creators, but also as a *quid pro quo* aimed at ensuring both protections for creators and public access to creative works. As the Court put it:

subject to a number of enumerated exceptions.[28] First among these is the exception for fair use of copyrighted works.[29]

Unlike many of the other limitations upon copyright holders' exclusive rights, the fair use exception is not limited to particular categories of works or users. Indeed, the exception is conspicuously open-ended in at least two respects. First, it specifies illustrative categories of uses that will be deemed "fair," rather than enumerating specific facts that must be present to claim the exception.[30] Second, the statute aims to guide, instead of limit, the exercise of judicial discretion by enumerating four non-exclusive factors that courts should consider in resolving any proffered fair use defense.[31]

Whole books have been written on the subject of fair use,[32] and it is not my aim herein to provide more than a broad outline of the doctrine. Certain features common to fair uses in general, however, are particularly salient to a consideration of fair use in the digital domain.

First, fair uses are *unauthorized by the copyright holder*. That is to say, the would-be fair user of copyrighted material need not obtain the copyright holder's approval to do so; to the contrary, fair uses are

---

> The limited scope of the copyright holder's statutory monopoly, like the limited copyright duration required by the Constitution, reflects a balance of competing claims upon the public interest: Creative work is to be encouraged and rewarded, but private motivation must ultimately serve the cause of promoting broad public availability of literature, music, and the other arts.

Twentieth Century Music Corp. v. Aiken, 422 U.S. 151, 156 (1975) (footnotes omitted).

28. *See* 17 U.S.C. §§ 107–122 (2000).

29. *Id.* § 107.

30. *Id.* (referring to permissibility of copying "for purposes such as criticism, comment, news reporting, teaching (including multiple copies for classroom use), scholarship, or research").

31. *Id.* Courts must consider:

> (1) the purpose and character of the use, including whether such use is of a commercial nature or is for nonprofit educational purposes; (2) the nature of the copyrighted work; (3) the amount and substantiality of the portion used in relation to the copyrighted work as a whole; and (4) the effect of the use upon the potential market for or value of the copyrighted work.

Id. In construing this provision, the Supreme Court has cautioned that the fair use inquiry "is not to be simplified with bright-line rules, for the statute, like the doctrine it recognizes, calls for case-by-case analysis . . . . [The factors] provide only general guidance about the sorts of copying that courts and Congress most commonly had found to be fair uses." Campbell v. Acuff-Rose Music, Inc., 510 U.S. 569, 577–78 (1994). Commentators have suggested that the statute by its terms authorizes the courts to consider the inherent equity of any given use — to reason, in other words, that its innate "fairness" or "unfairness" may authorize, or forbid, a use irrespective of precisely how the enumerated statutory factors are balanced. *See* Lloyd L. Weinreb, *Fair's Fair: A Comment on the Fair Use Doctrine*, 103 HARV. L. REV. 1137, 1150 (1990) ("Fair use does not exclude consideration of factors not related to the utilitarian justification for copyright — other social values or, more simply, fairness."). Certainly the reported cases on fair use do not appear to be dictated solely by consideration of the four statutory factors. *See* Nimmer, *supra* note 10, at 267.

32. *See, e.g.*, WILLIAM F. PATRY, THE FAIR USE PRIVILEGE IN COPYRIGHT LAW (2d ed. 1995); FAIR USE AND FREE INQUIRY: COPYRIGHT LAW AND THE NEW MEDIA (John Shelton Lawrence & Bernard Timberg eds., 1989).

lawful even where permission has been sought and denied.[33] As a policy matter, the protection of fair use is likely to be most necessary where, as with the vulgar parody in *Campbell v. Acuff-Rose Music*,[34] the copyright holder withholds permission in the face of criticism or parody, no matter what licensing fee a user might offer. By protecting such uses irrespective of the copyright holder's wishes, the fair use doctrine contributes to the creation of works that would not exist if the copyright holder's denial of permission were dispositive.

Second, fair uses *do not require compensation* to the copyright holder. Just as the copyright holder is not empowered to authorize or reject a fair use, so too is the user excused from any requirement to pay the copyright holder in order to exercise fair use rights. One could imagine a system in which any user could make any use of any work they wished so long as that user paid a compulsory royalty to the copyright holder.[35] The fair use doctrine does not establish such a system, but rather withdraws from copyright holders the right to insist upon compensation for fair uses.[36]

Third, and perhaps in consequence of the two features already named, most offline fair uses *are effectively anonymous*. Because the user need not alert the copyright holder to the use, either to obtain permission or to arrange for payment, most users will not alert the copyright holder at all when making a use they believe is fair. Al-

---

33. *See Campbell*, 510 U.S. at 572–73.

34. *Id.*

35. *See, e.g.*, 17 U.S.C. § 115 (2000) (establishing compulsory licensing scheme allowing any person, upon payment of a statutory royalty, to make a recording of a nondramatic musical work that has previously been recorded, so long as "the basic melody or fundamental character of the work" is not changed).

36. *Cf.* Wendy J. Gordon, *Fair Use as Market Failure: A Structural and Economic Analysis of the Betamax Case and its Predecessors*, 82 COLUM. L. REV. 1600, 1614–15 (1982) (arguing that breakdown in the market for licensing uses of the copyrighted work is a factor that would-be fair users ought to be required to demonstrate to take advantage of the fair use doctrine). Limiting fair use to circumstances where market approaches fail, however, cedes to copyright holders the sole authority to define (by refusing to offer a license) which uses are fair — a greater measure of control than the fair use doctrine actually provides. For that reason, it seems preferable to characterize the fair use doctrine as withdrawing a subset of possible uses from the domain of licensing altogether, instead of limiting fair use to those circumstances where the copyright holder elects not to offer a license.

This approach finds support in case law, particularly in the recognition by some courts that the fourth statutory fair use factor is susceptible to manipulation by copyright holders who may try to create the appearance of adverse market effects by offering to license their works for uses that would otherwise be recognized as fair. Although some courts have shown sensitivity to the risk that these tactical licensing decisions may curtail fair uses by magnifying the appearance of forgone licensing revenues, others have apparently allowed such artificially created market effects to weigh against a finding of fair use. *Compare* Bill Graham Archives v. Dorling Kindersley Ltd., 448 F.3d 605, 614–15 (2d Cir. 2006) (cautioning against giving dispositive weight in assessment of market effects to copyright holder's licensing decisions) *with* Perfect 10 v. Google, Inc., 416 F. Supp. 2d 828, 832, 851 (C.D. Cal. 2006) (rejecting fair use defense when plaintiff had licensed its own works for transformative purposes after commencement of litigation and alleged fair use would harm potential market for these licensed works).

though copyright holders may nevertheless come to learn of the use, particularly where the use is highly public or involves large-scale copying,[37] as a practical matter, fair uses tend to occur "under the radar" of copyright holders and are essentially anonymous.

The fair use doctrine as it exists in traditional copyright law, accordingly, protects users' rights to make *unauthorized, uncompensated, and effectively anonymous* copies of a copyrighted work for purposes such as those given in the statute.[38] As will be discussed in this Article, much of the difficulty with implementing the fair use doctrine in the digital domain revolves around the problematic representation of these features of traditional fair use law through DRM.

These contours of traditional copyright law provide a baseline of common user experiences with copyrighted works against which DRM systems may be compared. The fair use doctrine imparts to users a reasonable belief that they may engage, without fear of liability, in uses of copyrighted content of the sort that have been found to be fair. The evolution of DRM, however, demonstrates how technological and legal measures have combined to frustrate these settled user expectations.[39]

B. Contemporary Copyright: DRM as a "Speedbump" to Slow Mass Infringement[40]

In the 1990s, the combination of advancing compression technologies, wide availability of desired entertainment products in easily reproducible digital form, increasing computer power and storage capacity, and growing access to the Internet at broadband speeds formed

---

37. *See, e.g.*, Princeton Univ. Press v. Mich. Document Servs., Inc., 99 F.3d 1381, 1384 (6th Cir. 1996) (en banc); Basic Books, Inc. v. Kinko's Graphics Corp., 758 F. Supp. 1522, 1526 (S.D.N.Y. 1991).

38. A separate characteristic might be ascribed to many fair uses: because advance permission need not be sought and compensation need not be paid, users may make *spontaneous* fair uses of a copyrighted work. Preserving spontaneous fair use involves a technical challenge for DRM systems. Fair use protection, however, applies irrespective of spontaneity — that is to say, the doctrine remains equally applicable even if it is necessary, for example, to retrieve the work from a remote library before it may be used. Spontaneity, therefore, is merely one consequence of the rule that the copyright owner's permission is not required for fair use. The doctrine permits fair use even where there would be adequate time to secure the copyright holder's permission were the parties inclined to negotiate.

39. *See* Deirdre Mulligan & Aaron Burstein, *Implementing Copyright Limitations in Rights Expression Languages*, *in* DIGITAL RIGHTS MANAGEMENT: ACM CCS-9 WORKSHOP, DRM 2002, LNCS 2696, at 137, 139 (Joan Feigenbaum ed., 2003), *available at* http://www.law.berkeley.edu/clinics/samuelson/projects_papers/2002f_drm_acm_paper.pdf ("Machine-enforced use restrictions . . . frequently defy the 'real space norms' that have developed around the use of copyrighted works."); *see also infra* notes 175–78 and accompanying text.

40. *See generally* Digital Media Project, Berkman Center for Internet & Society at Harvard Law School, Speedbumps Scenario for Digital Media, http://cyber.law.harvard.edu/media/scenario2 (last visited Nov. 16, 2006).

a "perfect storm."[41] It supplied the conditions for a fundamental unsettling of the incumbent balance between end users' ability to redistribute copyrighted content and copyright holders' ability to limit such redistribution.[42] These changes created a crisis of confidence for digital media copyright holders. Their response was twofold. First, they deployed technological protection measures, including rudimentary encryption systems, to control access to authorized media. These measures, however, were recognized from the outset to be vulnerable to circumvention by sophisticated users, who might circulate copies of the content from which the DRM mechanisms had been stripped. Accordingly, copyright holders took the second step of seeking special legal protections for DRM mechanisms. The World Intellectual Property Organization ("WIPO") adopted treaties that mandated stronger statutory protections for DRM in signatory nations,[43] and Congress responded by enacting the DMCA.[44]

1. Digital Rights Management

Federal law provides heavy penalties for copyright infringement.[45] The fear of liability, of course, suffices to deter at least some would-be infringers. DRM technologies attempt to go one step further by making copyright infringement impractical or costly.[46] DRM, properly deployed, provides a second level of deterrence that prevents at least some violations committed by users not adequately deterred by the fear of legal liability. What makes DRM controversial is its potential to overdeter — to prevent lawful, noninfringing uses of protected content.[47]

---

41. *See, e.g.*, Richard Owens & Rajen Akalu, *Legal Policy and Digital Rights Management*, 92 PROC. IEEE 997, 997 (2004) ("Duplication of content has, thus, become easy, cheap, and perfect. Acquisition of duplicated content has become nearly instantaneous and free."); FISHER, *supra* note 4, ch. 3.

42. *See, e.g.*, Owens & Akalu, *supra* note 41, at 997; FISHER, *supra* note 4, ch. 3.

43. World Intellectual Property Organization, WIPO Copyright Treaty art. 11, Dec. 20, 1996, S. Treaty Doc. No. 105-17, at 1 (1997), 36 I.L.M. 65, *available at* http://www.wipo.int/treaties/en/ip/wct/trtdocs_wo033.html [hereinafter WIPO Copyright Treaty]; World Intellectual Property Organization, WIPO Performances and Phonograms Treaty art. 18, Dec. 20, 1996, S. Treaty Doc. No. 105-17, at 18 (1997), 36 I.L.M. 76, *available at* http://www.wipo.int/treaties/en/ip/wppt/trtdocs_wo034.html [hereinafter WIPO Performances and Phonograms Treaty].

44. *See supra* note 4 and accompanying text.

45. *See* 17 U.S.C. § 501 (2000 & Supp. 2002). Civil remedies include statutory damages of up to $30,000 per infringing act, which increase to $150,000 if the infringement is found to be willful. *Id.* § 504(c). Criminal penalties are available where the infringer profited, where the total retail value of the infringed works exceeded $1,000, or where the infringer leaked a pre-release copy of a copyrighted work on the Internet. *Id.* § 506(a).

46. For a more sophisticated assessment of the behavioral incentives underlying the adoption of DRM technologies and the use of DRM-protected products, see John A. Rothchild, *Economic Analysis of Technological Protection Measures*, 84 OR. L. REV. 489 (2005).

47. *See supra* note 5 and accompanying text.

The technological debate over DRM revolves around the issue of efficacy.[48] The present situation is difficult to define except in broad generalizations. Copyright holders' deployment of DRM technologies sparked an ongoing "arms race" of sorts, with each successive technological advance on one side being met by a response on the other.[49] That race continues. Of technological measures deployed to protect digital music, (1) attempts to embed protection measures in Compact Discs ("CDs") generally have a poor record of success, and (2) efforts to protect digital music files on the Internet against copying and unauthorized use have succeeded in the market in inverse proportion to the burden they place on users.

There have been many failed attempts to embed protection technologies into CDs. The most recent, and highly public, failure arose from an ill-considered attempt by Sony to embed DRM technologies in audio CDs. The DRM software Sony deployed shared a number of pernicious characteristics with so-called "spyware" and "rootkit" programs.[50] Sony CDs even damaged a number of users' computers, leaving them vulnerable to attack by malicious third-party software, before the company executed a public-relations about-face and offered to replace the affected CDs.[51]

Even before the Sony "rootkit DRM" fiasco, efforts to include DRM systems in audio CDs had failed repeatedly. The design of audio CD technology, which antedates widespread industry concern with copy protection, has been a significant factor in limiting the effective deployment of DRM systems. The "Red Book" technical standards for audio CDs lack any provision allowing for encryption of the

---

48. *See, e.g.*, Fred von Lohmann, *Measuring the Digital Millennium Copyright Act Against the Darknet: Implications for the Regulation of Technological Protection Measures*, 24 LOY. L.A. ENT. L. REV. 635, 640–41 (2004) (arguing that technological measures to date have proven ineffective at preventing mass copying and distribution of DRM-protected works); *Felten Testimony*, *supra* note 3, at 2.

49. One dedicated Norwegian programmer, Jon ("DVD Jon") Johansen, has compiled a résumé that virtually encapsulates the major milestones in the battle between pro- and anti-DRM forces. As a teenager, Johansen co-wrote the "DeCSS" program that allowed users to decrypt the contents of encrypted DVD Video discs even if they had not paid a licensing fee for a lawful decryption key. *See* Universal City Studios, Inc. v. Corley, 273 F.3d 429, 437 (2d Cir. 2001). More recently, Johansen has written software to bypass the DRM protection of songs offered for sale on Apple Computer's iTunes Store — and rewritten it in response to Apple's efforts to bypass Johansen's software. *See* Wikipedia, *Jon Lech Johansen*, http://en.wikipedia.org/wiki/Jon_Lech_Johansen (as of Nov. 16, 2006, 21:28 GMT). Johansen has also registered the Internet domain name "DeAACS.com" as he plans to work on a program to bypass the protections of the Advanced Access Content System for next-generation DVDs. Dan Bell, Jon Lech Johansen Creator of DeCSS Registers DeAACS Domain (Jan. 15, 2006), http://www.cdfreaks.com/news/12948; *see also infra* note 67.

50. *See* Lorraine Woellert, *Sony BMG Ends a Legal Nightmare*, BUS. WK. ONLINE, Dec. 20, 2005, http://www.businessweek.com/technology/content/dec2005/tc20051230_658336.htm.

51. *See id.*; J. Alex Halderman & Edward W. Felten, Lessons from the Sony CD DRM Episode: Extended Version (Feb. 14, 2006), http://itpolicy.princeton.edu/pub/sonydrm-ext.pdf.

disc's audio content.[52] Because copyrighted content is released on audio CDs in unprotected form, it has been particularly susceptible to the development of technologies that facilitate digital copying.[53] Efforts to alter the audio CD format to incorporate copy protections, however, have met with resistance on a number of fronts. First, consumers have balked due to the incompatibility of copy-protected CDs with existing player hardware — an incompatibility that in some cases actually damaged consumers' equipment.[54] Second, the licensor of the official Compact Disc specification has refused to allow nonconforming discs to bear the trademarked "Compact Disc" logo.[55] Finally, Congress has considered truth-in-advertising legislation that would require prominent warning labels on the packaging of copy-protected audio CDs.[56]

The most ambitious effort to develop new copy-protection technologies for digital audio ended in a highly publicized meltdown. The proponents of the Secure Digital Music Initiative ("SDMI") offered a $10,000 prize to anyone who could "break" the digital watermarking technology they had developed — a task that was accomplished in approximately three weeks by a team of researchers led by Princeton University computer scientist Edward Felten.[57] Felten's team rejected the proffered cash reward and elected instead to publish the results of their research, although not before fending off a threatened lawsuit from SDMI and its affiliates.[58]

Where DRM technology has been implemented to protect digital audio recordings, its success in the marketplace has varied depending on its impact on users. Attempts by the music industry to fill the post-Napster void to make digital music available have employed, for the most part, highly restrictive DRM protections. For example, MusicNet, an early joint venture between recording industry participants Bertelsmann, EMI, and Time Warner, initially prohibited users from actually downloading songs to the user's hard drive.[59] Instead, in ex-

---

52. *See* Wikipedia, *Compact Disc*, http://en.wikipedia.org/wiki/Compact_disc (as of Nov. 16, 2006, 21:38 GMT).

53. *See* FISHER, *supra* note 4, at 83.

54. *See Dion's CD Can Crash PCs*, BBC NEWS, Apr. 5, 2002, http://news.bbc.co.uk/2/hi/entertainment/1912466.stm; Barry Willis, *Copy-Protected CDs a Nightmare for BMG Germany*, STEREOPHILE, Feb. 6, 2000, http://www.stereophile.com/news/10671/index.html.

55. *See* Wikipedia, *Compact Disc*, *supra* note 52.

56. *See* Digital Media Consumers' Rights Act of 2005, H.R. 1201, 109th Cong. (1st Sess. 2005), *available at* http://www.boucher.house.gov/images/stories/Documents/copy_bill_1201.pdf.

57. *See* Scott A. Craver et al., Reading Between the Lines: Lessons from the SDMI Challenge (2001), http://www.usenix.org/publications/library/proceedings/sec01/craver.pdf (published results of Felten's research); FISHER, *supra* note 4, at 89, 96–97.

58. *See* FISHER, *supra* note 4, at 96–97.

59. *See* Michael Bertin, *After Napster*, AUSTIN CHRON., Aug. 17, 2001, at 56, *available at* http://www.austinchronicle.com/issues/dispatch/2001-08-17/music_feature.html; Reggie

change for a monthly subscription fee, users were allowed to stream a given number of songs from the participants' catalogs; this essentially required users to listen to the songs at their computer, rather than allowing them to transfer the songs to a portable player or burn them to an audio CD.[60]

In contrast, Apple Computer's iTunes Music Store ("iTMS"),[61] launched with great fanfare in 2003, became notable in part because of the relatively permissive terms enforced by its DRM software.[62] The iTMS became a major success with users, capturing seventy percent of the U.S. market for authorized online music just a year after its debut.[63] The iTMS employs DRM software known as "FairPlay" to limit redistribution and copying of content downloaded from iTMS.[64] The success of iTMS supports the assertion that online digital audio providers succeed in the market in inverse proportion to the level of protective restrictions they place on users.

Technological protection measures for video content such as feature films have arguably fared better. The combination of region coding and a rudimentary encryption scheme for DVD Video discs is ubiquitous today, even though the technology proved from the outset to be easily circumvented.[65] DRM mechanisms remain highly relevant

---

Beehner, *Web Music Gets Legal (and Less Flexible)*, PC WORLD, May 17, 2001, http://www.pcworld.com/news/article/0,aid,50344,00.asp.

60. *See* Bertin, *supra* note 59; Beehner, *supra* note 59. Other services charge extra for the ability to burn a song to a CD. *See, e.g.*, Rhapsody: FAQs & Help, http://www.listen.com/faq.jsp (last visited Nov. 16, 2006).

61. Apple Computer changed the name from iTunes Music Store to iTunes Store on September 12, 2006. *See* Wikipedia, *iTunes Store*, http://en.wikipedia.org/wiki/ITunes_Store (as of Nov. 16, 2006, 22:01 GMT).

62. *See* Wikipedia, *FairPlay*, http://en.wikipedia.org/wiki/FairPlay (as of Nov. 16, 2006, 22:02 GMT). FairPlay does have certain constraints, however, such as the limitation that the only portable digital music player on which music purchased from iTMS can be played is the Apple iPod. *See id.*

63. *See* Darren Waters, *Europe Launch for Apple's iTunes*, BBC NEWS, June 15, 2004, http://news.bbc.co.uk/2/hi/entertainment/3805565.stm.

64. *See* Wikipedia, *FairPlay*, *supra* note 62. For an examination of the crucial role DRM technology plays in enabling Apple's iTMS business model, see Digital Media Project, The Berkman Center for Internet & Society at Harvard Law School, iTunes: How Copyright, Contract, and Technology Shape the Business of Digital Media — A Case Study, 40–48 (2004), http://cyber.law.harvard.edu/media/itunes.

65. The "Content Scramble System" ("CSS") encrypts the audiovisual content of a DVD disc using a rudimentary forty-bit stream cipher, which is much weaker than the type of encryption commonly used, for example, to protect online financial transactions. *See* Ananda Gupta, The DeCSS Mess: A Study in Unintended Consequences (Aug. 31, 2000), http://www.cei.org/gencon/016,01836.cfm; Jeffrey A. Bloom et al., *Copy Protection for DVD Video*, 87 PROC. IEEE 1267 (1999). Because of the apparent vulnerability of the CSS algorithm, experts question "[w]hether CSS is a serious cryptographic cipher." Frank A. Stevenson, Cryptanalysis of Contents Scrambling System (Nov. 8, 1999), http://www.cs.cmu.edu/~dst/DeCSS/FrankStevenson/analysis.html. Indeed, CSS was broken by a teenaged computer programmer in 1999, and the de-scrambling code was posted online in the form of a program called "DeCSS." *See supra* note 49. Nevertheless, the CSS DRM mechanism, together with a region coding scheme that nominally limits DVDs to playback in certain countries or regions of the globe, has remained an integral part of au-

and topical in the digital video context, with applications as varied as digital television broadcasting[66] and high-definition video discs.[67] Indeed, concern over copyright infringement in video works has led to the introduction of legislation mandating the inclusion of specified DRM technologies in any device capable of converting between analog and digital video formats — an effort to plug what has become known as the "analog hole."[68]

Because of the risk that, once a DRM system has been "broken," the underlying content may be broadly circulated in unprotected form, some observers have concluded that DRM is a futile endeavor.[69] Although some have suggested that the problem may be avoided by designing break once, break everywhere ("BOBE")-resistant DRM systems,[70] others have expressed doubt whether such systems can ever be made practical.[71]

---

thorized DVD releases to the present. *See* Wikipedia, *DVD*, http://en.wikipedia.org/wiki/Dvd (as of Nov. 16, 2006, 22:09 GMT).

66. In *American Library Ass'n v. FCC*, 406 F.3d 689 (D.C. Cir. 2005), the Court of Appeals struck down an FCC regulation that would have outlawed the domestic sale of digital television receiver hardware that did not include a particular DRM scheme — the so-called "broadcast flag" — designed to prevent unauthorized duplication of digital video content. For an overview of the implications of the decision, see Cuong Lam Nguyen, *A Postmortem of the Digital Television Broadcast Flag*, 42 HOUS. L. REV. 1129 (2005). The specific issue of the broadcast flag is sure to recur in other contexts. Also, attempts to read *American Library Ass'n* as a broad limitation on the reach of the FCC's regulatory power likely must be rethought in the wake of *National Cable & Telecommunications. Ass'n v. Brand X Internet Services*, 545 U.S. 967 (2005), in which the Supreme Court applied *Chevron* deference to an FCC ruling.

67. The developers of both formats vying to replace the DVD Video disc — HD-DVD and Blu-Ray — have settled on a common DRM mechanism, the Advanced Access Content System ("AACS") that both types of discs will employ. *See* Wikipedia, *Advanced Access Content System*, http://en.wikipedia.org/wiki/Advanced_Access_Content_System (as of Nov. 16, 2006, 22:10 GMT).

68. Digital Transition Content Security Act of 2005, H.R. 4569, 109th Cong. (1st Sess. 2005). For a skeptical appraisal of the bill and the term "analog hole" in general, see Edward W. Felten, The Professional Device Hole (Jan. 12, 2006), http://www.freedom-to-tinker.com/?p=954.

69. *See, e.g.*, Cory Doctorow, Microsoft Research DRM Talk (June 17, 2004), http://craphound.com/msftdrm.txt ("At the end of the day, all DRM systems share a common vulnerability: they provide their attackers with ciphertext, the cipher and the key."); Edward W. Felten, DMCA, and Disrupting the Darknet (Aug. 17, 2005), http://www.freedom-to-tinker.com/?p=889 ("Files arrive on the darknet having already been stripped of any technological protection measures . . . . And you can't circumvent a TPM that isn't there."); *see also supra* note 3.

70. Some authors have described the desired capability of DRM schemes to resist attack as follows:

> DRM systems strive to be BOBE (break once, break everywhere)-resistant. That is, suppliers anticipate that individual instances (clients) of all security systems, whether based on hardware or software, will be subverted. If a client of a system is subverted, then all content protected by that DRM client can be unprotected. If the break can be applied to any other DRM client of that class so that all of those users can break their systems, then the DRM-scheme is BOBE-weak. If, on the other hand, knowledge gained breaking one client cannot be applied elsewhere, then the DRM system is BOBE-strong.

The efficacy of any DRM measure is determined only partly by technological constraints. Also important are the freedoms the DRM mechanism presents to end users of the protected content. Other things being equal, users prefer alternatives that maximize flexibility in use of the content.[72] Content that can be accessed from multiple locations and multiple devices is more attractive than content that is tethered to a particular location or device. If DRM mechanisms interfere with user preferences in the manner of use of the underlying content, users are more likely to "cheat" — to circumvent the DRM protections — in order to obtain unfettered access to the protected content.[73] Recognition that technological measures alone are unlikely to be sufficient to deter infringement has spurred copyright industry representatives to seek stronger legal protections for DRM mechanisms.

2. Anti-Circumvention Restrictions

Content providers lobbied in the mid-1990s for the passage of international measures dealing with DRM circumvention, and were rewarded in 1996 with the adoption of two new copyright treaties by WIPO. Article 11 of the WIPO Copyright Treaty ("WCT") required signatory nations, including the United States, to

> provide adequate legal protection and effective legal remedies against the circumvention of effective technological measures that are used by authors in connection with the exercise of their rights under this Treaty or the Berne Convention and that restrict acts, in respect of their works, which are not authorized by the authors concerned or permitted by law.[74]

Peter Biddle et al., *The Darknet and the Future of Content Distribution*, *in* DIGITAL RIGHTS MANAGEMENT: ACM CCS-9 WORKSHOP, DRM 2002, LNCS 2696, at 155, 169 (Joan Feigenbaum ed., 2003); *see also* Markus Schneider & Anders Henten, *DRMS and TCP: Technology and Law* 5 (CTI Working Papers No. 76, 2003), *available at* http://www.dtu.dk/upload/centre/cict/publications/working%20papers/ctiwp76.pdf.

71. *See, e.g.*, Ryan Roemer, *Locking Down Loose Bits: Trusted Computing, Digital Rights Management, and the Fight for Copyright Control on Your Computer*, 7 UCLA J.L. & TECH. 8, 8 (2003), http://www.lawtechjournal.com/articles/2003/08_040223_roemer.pdf.

72. *See supra* notes 61–64 and accompanying text.

73. *See* Rachna Dhamija & Fredrik Wallenberg, *A Framework for Evaluating Digital Rights Management Proposals*, *in* PROCEEDINGS OF THE FIRST INTERNATIONAL MOBILE IPR WORKSHOP: RIGHTS MANAGEMENT OF INFORMATION PRODUCTS ON THE MOBILE INTERNET 13, 14 (Olli Pitkänen ed., 2003), *available at* http://www.hiit.fi/publications/pub_files/mobileipr2003-2.pdf (arguing that "DRM systems that artificially make a product either excludable or rival invite circumvention activities by end users (who realize that, if they could remove the technical barriers, the product is neither excludable nor rival)").

74. WIPO Copyright Treaty, *supra* note 43, art. 11.

The contemporaneously adopted WIPO Performances and Phonograms Treaty ("WPPT") included similar requirements.[75] Despite arguments that United States law already supplied the legal protections the WCT and WPPT demanded, Congress ultimately concluded that new legislation was required to implement these treaty obligations. Congress enacted new legal protections against circumvention of DRM mechanisms in the DMCA.[76] The DMCA puts legal weight behind privately developed technological mechanisms for limiting unauthorized distribution of digital content by prohibiting both the circumvention of access control measures[77] and the trafficking of circumvention devices.[78] By outlawing circumvention and circumvention devices, the DMCA arguably improves the efficacy of DRM measures and inhibits copyright infringement.

Several provisions of the statute are aimed at boosting the efficacy of DRM mechanisms. First, the DMCA's anti-circumvention provision provides: "No person shall circumvent a technological measure that effectively controls access to a work protected under this title."[79] Second, the statute's anti-trafficking provision states:

> No person shall manufacture, import, offer to the public, provide, or otherwise traffic in any technology . . . that:
>
> (A) is primarily designed or produced for the purpose of circumventing a technological measure that effectively controls access to a work protected under this title;
>
> (B) has only limited commercially significant purpose or use other than to circumvent a technological measure that effectively controls access to a work protected under this title; or
>
> (C) is marketed by that person or another acting in concert with that person with that person's knowledge for use in circumventing a technological measure that effectively controls access to a work protected under this title.[80]

---

75. WIPO Performances and Phonograms Treaty, *supra* note 43, art. 18.

76. Pub. L. No. 105-304, 112 Stat. 2360 (1998) (codified as amended at 17 U.S.C. §§ 1201–1205 (2000)).

77. 17 U.S.C. § 1201(a)(1)(A).

78. *Id.* § 1201(a)(2).

79. *Id.* § 1201(a)(1)(A).

80. *Id.* § 1201(a)(2).

Finally, a third provision of the statute forbids production or trafficking in devices that circumvent any "technological measure that effectively protects a right of a copyright owner" in specified circumstances.[81]

3. Fair Use and the DMCA

The DMCA's prohibitions against both DRM circumvention and the creation of circumvention devices potentially erode the protections in U.S. copyright law allowing fair use of copyrighted works. Where digital content is protected by a DRM wrapper (even a trivial one, as in the case of CSS) and none of the DMCA's exceptions apply, circumventing the DRM may violate the DMCA even if the use of the accessed content would be protected under the fair use doctrine.

The tension between the DMCA and the fair use provisions of copyright law is not commanded by the statutory text or history. To the contrary, there are indications that the provisions were intended to coexist harmoniously. First, the DMCA's anti-circumvention rules were adopted to implement Article 11 of the WCT. That Article obliges member states to protect DRM mechanisms against circumvention when the use of the work is "not authorized by the authors concerned *or permitted by law*."[82] Fair use of copyrighted works is expressly "permitted by law" in the United States. Accordingly, a statutory prohibition on circumventing DRM that hinders fair use goes well beyond the requirements of the WCT. Second, the DMCA itself purports to preserve fair use rights in DRM-protected copyrighted works.[83]

Early judicial interpretations of the DMCA, however, found that the anti-circumvention provisions overrode the protections for fair use in the general copyright statute. In *Universal City Studios, Inc. v. Reimerdes*, for example, the court considered whether the fair use doctrine supplied a defense against alleged violations of the DMCA's anti-circumvention provisions.[84] The court noted that the DMCA included a number of explicit exceptions to the anti-circumvention provisions, but that fair use was not among the exceptions listed.[85] The court reasoned that the legislature's omission of an explicit provision allowing DRM circumvention for fair use meant that fair use provided

81. *Id.* § 1201(b)(1)(C).

82. WIPO Copyright Treaty, *supra* note 43, art. 11 (emphasis added).

83. 17 U.S.C. § 1201(c)(1) ("Nothing in this section shall affect rights, remedies, limitations, or defenses to copyright infringement, including fair use, under this title.").

84. Universal City Studios, Inc. v. Reimerdes, 111 F. Supp. 2d 294, 321–24 (S.D.N.Y. 2000), *aff'd sub nom.* Universal City Studios, Inc. v. Corley, 273 F.3d 429 (2d Cir. 2001).

85. *Id.* at 322–23.

no defense to an alleged violation of the DMCA.[86] The Court of Appeals rejected the defendants' argument that an implicit "fair use exception" to the DMCA was constitutionally required under First Amendment principles.[87]

Judicial glosses on the DMCA, accordingly, appear to prohibit circumvention of DRM mechanisms, even if the purpose of circumvention is to engage in a fair use of the underlying content. This prohibition prevents the DMCA from fulfilling one of its purposes, for it creates incentives to break the law to engage in fair use. A legal and technological structure for DRM that preserves the right and opportunity to make fair use of copyrighted works would align the law and users' incentives in a way that the DMCA, as presently construed, does not. As will be seen, however, most existing and proposed DRM mechanisms, even those purportedly designed with fair use in mind, may poorly serve users' interests.

III. TECHNOLOGICAL ACCOMMODATION FOR FAIR USE IN MODERN DRM SYSTEMS

A. Local Authorization

1. Rights Management Architecture

In the most common type of contemporary DRM mechanism, the decision whether to allow or deny a requested use of the DRM-protected content occurs at the local end user level.[88] User permis-

86. *Id.*; *see also id.* at 324 ("The fact that Congress elected to leave technologically unsophisticated persons who wish to make fair use of encrypted copyrighted works without the technical means of doing so is a matter for Congress . . . ."); RealNetworks, Inc. v. Streambox, Inc., No. 2:99CV02070, 2000 WL 127311, at *8 (W.D. Wash. Jan. 18, 2000) (rejecting possible fair use defense to alleged DMCA violation).

87. *Corley*, 273 F.3d at 458 (2d Cir. 2001). On this point, the *Corley* panel's decision may carry less force in the wake of *Eldred v. Ashcroft*, 537 U.S. 186 (2003). In finding that the Copyright Term Extension Act did not violate the First Amendment, the Supreme Court noted that "copyright law contains built-in First Amendment accommodations," including the fair use defense. *Id.* at 219–20; *see also* Stephen M. McJohn, Eldred*'s Aftermath: Tradition, the Copyright Clause, and the Constitutionalization of Fair Use*, 10 MICH. TELECOMM. & TECH. L. REV. 95, 130–31 (2003) ("Under the *Eldred* analysis, the availability of fair use is central to the constitutional basis of copyright protection. Thus, fair use after *Eldred* . . . can now also be more explicitly used to protect First Amendment values.") (footnotes omitted).

88. My focus in this section and those that follow is on the locus of the authorization decision that determines whether a given attempt to use DRM-protected content will succeed or fail. To be sure, even DRM mechanisms that make the authorization decision wholly at the local user level may be designed to communicate or share information with other parties, for ends that may or may not be benign. For a discussion of some of the possible types of information sharing that might occur even in a system designed to make authorization decisions at the local level, see Edward W. Felten, Google Video and Privacy (Jan. 20, 2006), http://www.freedom-to-tinker.com/?p=956.

sions are encoded directly into the purchased content or accompanying metadata. The CSS technology protecting DVD video discs typifies one such system: by purchasing a licensed DVD player and a DVD, the user acquires all the pieces necessary for the authorization mechanism to function. It is unnecessary for the user, or the user's hardware, to communicate with any outside authority in order to decrypt the CSS-protected content on the disc.[89] The CSS authorization process takes place at the point of use between the encoded disc and the user's DVD player, without the involvement of any external decisionmaker.[90]

Local authorization offers users several advantages. For one, digital media that contains all the information necessary for its own decryption is highly portable, because users do not need to maintain a network connection at the point of use. Another advantage is that no user-identifying information need be disclosed to obtain local authorization, so this type of system preserves anonymity — one of the defining characteristics of fair use in the offline domain.[91]

CSS is a relatively simple DRM mechanism that exists for the limited purpose of ensuring that DVD video discs are played on a licensed DVD player. Other DRM mechanisms, however, are based on Rights Expression Languages ("RELs") capable of modeling far more sophisticated sets of user permissions at the local level. One such system that has achieved widespread use is the "eXtensible rights Markup Language" ("XrML"), billed as "the digital rights language for trusted content and services."[92] XrML describes grants of rights to end users using markup tags based on the Extensible Markup Language ("XML"). XrML allows rights holders to specify particular uses of their content that are to be permitted, to limit grants of rights to particular users or classes of users, to place time or geographical limitations on exercise of the rights granted, and to condition exercise of the rights granted on the user's compliance with one or more preconditions such as the payment of a subscription or per-use fee.[93] In-

89. DVD discs differ in this regard from DIVX, a now-forgotten early competitor of DVD technology in the 120mm disc form factor. DIVX employed a subscription-plus-rental model in which it was necessary for the user's player to contact a remote server to obtain authorization to play a disc. *See infra* note 115 and accompanying text.

90. *See generally Corley*, 273 F.3d at 436–37 (explaining CSS authorization mechanism); JIM TAYLOR, DVD DEMYSTIFIED 192–93 (2d ed. 2001).

91. *See supra* Part II.A. *But cf. supra* note 88 (explaining how user anonymity could be compromised even when authorization decisions are made at the user level).

92. About XrML, http://www.xrml.org/about.asp (last visited Nov. 16, 2006). For recognition that XrML is sufficiently widespread to amount to a *de facto* standard, see, for example, Daniel Benoliel, *Technological Standards Inc.: Rethinking Cyberspace Regulatory Epistemology*, 92 CAL. L. REV. 1069, 1095 n.103 (2004) ("[A]mong the programming languages with the widest installed base [is] . . . eXtensible rights Markup Language (XrML) 2.0.

93. *See* About XrML, *supra* note 92.

telligently combining these various functionalities may allow rights holders to define grants of rights with great sophistication and detail.[94]

2. Protections for Fair Use

Despite their flexibility, DRM systems that rely entirely on local authorization may not effectively protect fair use rights. A review of some of the proposals to add protections for fair use to such systems reveals inherent shortcomings of the local authorization approach.

Two authors suggested modeling a useful subset of fair use rights in a DRM mechanism as "generalized grants from Congress" of permissions to use content in specified ways.[95] The rights they proposed to model, however, fall well short of the uses typically recognized as fair under federal copyright law. They initially proposed encoding into every DRM system a right to make one copy of a digital work for personal use, conditioned on prior authentication by specialized hardware components:

> A possible starting place for the set of permissions first designated as residing within the safe harbor might be to permit a single copy of a digital work (exclusively for personal use) to a designated and verifiable network of devices. The security and auditability of such a "personal domain" could be guaranteed by the required presence of a secure hardware component (such as a USB token or smart card) acquired via a license . . . . The problem — authenticating the copying device and ensuring that only one copy can be made — is clearly difficult but not insurmountable.[96]

---

94. I will cite XrML in the remainder of this article as a prototypical REL for local authorization DRM for simplicity and avoidance of duplicative examples. For another example of an influential XML-based REL, however, see The Open Digital Rights Language Initiative, http://odrl.net (last visited Nov. 16, 2006).

95. Barbara L. Fox & Brian A. LaMacchia, *Encouraging Recognition of Fair Uses in DRM Systems*, COMM. ACM, Apr. 2003, at 61, 63.

96. *Id.* The plan's reliance on secure hardware systems ("a designated and verifiable network of devices") might be a reflection of the fact that the authors were at the time employees of Microsoft Corporation, an advocate of "trusted systems" relying on closed, proprietary hardware made to inhibit free interoperability. *See, e.g.*, Wikipedia, *Next-Generation Secure Computing Base*, http://en.wikipedia.org/wiki/Next-Generation_Secure_Computing_Base (as of Nov. 16, 2006, 21:48 GMT). Market research, however, has consistently identified interoperability and media portability as important preconditions to consumer acceptance of DRM, suggesting that solutions based upon specialized hardware requirements may prove to be suboptimal. *See, e.g.*, Press Release, GartnerG2, GartnerG2 Says Digital Media Publishers Must Have Portable Digital Rights Management Standards or They Risk Alienating Consumers (Aug. 13, 2003), http://www.gartner.com/press_releases/pr13aug2003a.html. For a recent review of the development of interoperable DRM tech-

Recognizing the limitations of their proposal, the authors suggested that it was intended merely as a proof of concept for what "ultimately" may become "a series of expanding safe harbors for modeling larger and larger subsets of fair use rights in DRM systems."[97] The authors did not address what rights those future subsets may include or how they would be recognized in DRM mechanisms (particularly as to content previously issued under more restrictive DRM).

The design of XrML itself illustrates one of the chief difficulties of relying on locally authorized DRM mechanisms to protect fair use rights. XrML is a device for expressing grants of rights to access or use content in certain ways. One of the assumptions of an XrML-based DRM system is that such a grant of rights is necessary before the user may engage in the conduct specified in the grant. In operation, XrML checks the action the user wishes to take against the list of grants specified in the license or licenses applicable to the user.[98] If no matching grant is found in any license, the DRM system prevents the user from engaging in the requested use of the content.[99] In other words, in an XrML-based DRM system, *all uses not expressly permitted are forbidden*. The system denies permission by default; a user may engage in a use of the content only if the desired use has been encoded in the terms of the grant of rights.

In a DRM system that relies entirely on local authorization, this "deny by default" design impedes fair use by limiting the scope of available rights to those within the foresight of the original license issuer. Because the DRM prevents users from engaging in any uses not expressed *ex ante* in the grant, "[i]f fair use privileges and other legitimate interests of information users cannot be expressed in an REL, *such interests simply do not exist within the system*."[100]

Modeling the substantive law of fair use in a machine-executable XrML grant is difficult or impossible. The open-ended fair use definition in the federal copyright statute may be particularly ill-suited to reduction to an algorithm. Indeed, even a functional computer-administered fair use regime might noticeably contract the scope of rights that users presently enjoy. Princeton University computer scientist Edward Felten has recognized both of these problems:

---

nologies, see John Palfrey, *Holding Out for an Interoperable DRM Standard*, *in* DIGITAL RIGHTS MANAGEMENT: THE END OF COLLECTING SOCIETIES? 1 (Christoph Beat Graber et al. eds., 2005).

97. Fox & LaMacchia, *supra* note 95, at 63.

98. *See* XrML 2.0 Technical Overview 4 (Mar. 8, 2002), http://www.xrml.org/Reference/XrMLTechnicalOverviewV1.pdf.

99. *See id.*

100. Bechtold, *supra* note 7 (emphasis added); *see also* Fox & LaMacchia, *supra* note 95, at 61 ("Only actions explicitly authorized by content owners or their delegate(s) are allowed, and the only 'rights' are those explicitly granted by them and presented to the DRM system.").

> The legal definition of fair use is, by computer scientists' standards, maddeningly vague. No enumeration of fair uses is provided. There is not even a precise algorithm for deciding whether a particular use is fair. Instead, the law says that judges should make case-by-case decisions based on four factors . . . . The law does not say exactly how these factors should be evaluated or even how the factors should be weighted against one another.
>
> To a computer scientist, such imprecision is a bug; to lawyers it is a feature, since it allows judges to take into account the unique circumstances of each case. Making fair use a judgment call allows the fair use doctrine to evolve in light of technological innovation. It provides a kind of flexibility and adaptability that would not be possible with a more precisely specified rule.[101]

Professor Felten also highlighted the difficulty of providing any computer program with the information necessary to enable an *ex ante* decision regarding whether a given use is fair.[102] He then articulated the difficulty in designing an artificial-intelligence system sophisticated enough to mimic the sifting and weighing of a mass of complex and contradictory evidence that a human judge might undertake in evaluating the fairness of a given use:

> For instance, the fourth factor in the test evaluates the effect of the use on the market for the original work. It requires reasoning about the economics of a particular market, a task even well-trained humans find difficult. For the foreseeable future, no com-

---

101. Felten, *supra* note 9, at 58.

102. *See id.* (hypothesizing that a DRM system cannot know, for example, whether a given use is conducted in a classroom setting, which would weigh in favor of a finding of fair use); *see also* John S. Erickson & Deirdre K. Mulligan, *The Technical and Legal Dangers of Code-Based Fair Use Enforcement*, 92 PROC. IEEE 985, 986 (2004) (also noting the difficulty of describing fair use factors in machine-interpretable form). Although his general point is surely valid, Professor Felten's specific example may not be particularly forceful. *See*, *e.g.*, Séverine Dusollier, *Fair Use by Design in the European Copyright Directive of 2001*, COMM. ACM, Apr. 2003, at 51, 52 ("Fair use principles may be embedded in the design of technological protection measures; for example, the digital rights management system can acknowledge the individual requesting a copy of the work as a teacher, allowing this person to take a portion of the work for quotation."); ContentGuard, eXtensible rights Markup Language (XrML) Example Use Cases [hereinafter XrML Example Use Cases] (on file with author) (giving many examples of coding special permissions for academic use in XrML).

> puter system will be able to approach a human's ability to analyze these markets.[103]

Legal commentators have expressed the same skepticism as Professor Felten that technological means alone can achieve an adequate *a priori* approximation of fair use doctrine:

> Building the range of possible uses and outcomes into computer code would require both a bewildering degree of complexity and an impossible level of prescience. There is currently no good algorithm that is capable of producing such an analysis. Relatedly, fair use is a dynamic, equitable doctrine designed to respond to changing conditions of use. Programmed fair use functionality, in contrast, is relatively static. 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.[104]

Other authors, too, have emphasized the technical complexities involved in reducing even a small subset of permissible fair uses to code before the actual circumstances giving rise to a claimed fair use are known.[105]

If the design of XrML itself makes accommodating fair use rights difficult,[106] might changing XrML solve the problem?[107] Proposed extensions to the language would make it easier to express fair use rights in XrML. One such extension is the addition of new default elements that allow, rather than restrict, certain uses for certain types

---

103. Felten, *supra* note 9, at 58. Of course, even human judges often render decisions that depart from the outcome expected by a reasonable consideration of the four statutory factors. *See* Nimmer, *supra* note 10, at 282.

104. Dan L. Burk & Julie E. Cohen, *Fair Use Infrastructure for Rights Management Systems*, 15 HARV. J.L. & TECH. 41, 56 (2001).

105. *See* Erickson & Mulligan, *supra* note 102, at 993 ("To accommodate even some approximation of actions that may be protected by fair use, authorities must somehow preauthorize a set of yet-unspecified actions that the user may invoke for yet-undefined purposes, which together will provide users with 'space' for fair use.").

106. *See, e.g.*, Bechtold, *supra* note 6, at 604 ("[M]ost current RELs do not provide ample tools to express how and under which conditions content may be reused, altered, reformatted, modified or otherwise transformed for the integration —be it in part or as a whole — into other works.").

107. It is not difficult, for example, to imagine an inverted XrML system requiring all *restrictions* on user freedom to be adequately and precisely described before being enforced — in other words, a system that would allow all uses except those specifically disallowed in the terms of the accompanying XrML code.

of protected content.[108] These changes, however, would likely necessitate the abandonment of XrML's assumed agnosticism regarding the type of media to which it is applied in a given case.[109] Even more ambitious proposals have suggested fundamental changes to XrML by challenging the language's "one-way" expression of rights. Under these proposals, the information flow of assertions about rights would run not only from the copyright holder to the user, but in the opposite direction as well. Such a change would require the addition of an expanded Rights Messaging Protocol ("RMP") to XrML to support the multidirectional assertion of rights, which would change the language in quite substantial ways.[110] The very breadth of the various proposals for revising XrML, however, confirms a much simpler point: at present, the language and the DRM mechanisms in which the language is employed are not optimal for recognizing and protecting end user fair use rights in digital content.

These difficulties are inherent to any DRM mechanism that relies wholly on local authorization at the end user level to resolve whether a user may engage in a desired use of the protected content. The impossibility of describing end user fair use rights *ex ante* in a form that can be interpreted and executed by machine — at least with precision even approaching the subtlety that a human decisionmaker might provide — suggests that the solution might be to "introduc[e] . . . an external decisionmaker into the process for obtaining access to technologically secured works."[111] As the next section discusses, however, the protection of end user fair use rights in such a system would present its own set of complications.

B. Remote Authorization

1. Rights Management Architecture

Some of the limitations on the sophistication of DRM decisionmaking that occurs entirely at the end user level might be avoided by relying instead on an outside authority to approve requested uses of the protected content. In such a remote authorization system, the user receives a protected digital file that contains a mechanism for contacting an outside authority to approve requests to use the content in certain ways, rather than a hard-coded description of preauthorized uses. When the user seeks to access or use the protected content, a DRM-compliant player program contacts a remote server to obtain authori-

108. *See, e.g.*, Samuelson Law, Tech. & Pub. Policy Clinic, Supporting Limits on Copyright Exclusivity in a Rights Expression Language Standard 11–12 (Aug. 13, 2002), http://xml.coverpages.org/OASIS-SLTPPC-EPIC-8-13-02.pdf.

109. *See infra* note 188 and accompanying text.

110. *See* Mulligan & Burstein, *supra* note 39, at 141; discussion *infra* Part IV.A.2.

111. Burk & Cohen, *supra* note 104, at 59.

zation for the use. If the authority for the requested use is granted, the player program allows the use; otherwise, it prevents access.

Remotely administered DRM mechanisms suffer from some undeniable practical disadvantages. Because any such system must be able to access a remote server to obtain authorization for any desired use, the system is inherently ill-suited for use with devices (such as portable music players) that lack built-in network connectivity. If the player is unable to access a licensing authority, the default — just as in an XrML-based DRM system — would be to deny the use. In regions where network connectivity is unreliable or costly, this may be a substantial drawback.[112] Where users access DRM-protected content with an appliance not ordinarily connected to a computer network (such as a stand-alone DVD player), redesigning the player appliance for network connectivity may introduce an additional level of cost and complexity that many users will find unappealing and that producers may find uneconomical.[113]

On the other hand, using an external decisionmaker in the authorization process may benefit users in other ways. By potentially allowing for human involvement, a remote authorization system permits, at least in principle, a greater level of complexity in the circumstances that may be considered. Supplying a technological framework for negotiation of usage rights may foster uses and transactions that could not have occurred with a less sophisticated DRM mechanism.

---

112. DIVX video disc technology, discussed *infra* note 115 and accompanying text, came — and went — during an era when most Americans relied on dial-up access to computer networks. It is interesting to speculate whether DIVX technology would have suffered the same fate had it instead evolved in an era of widespread, always-on broadband network access. It is possible that the factors sometimes offered to explain DVD's success — such as users' putative preferences for owning rather than renting content — would not have proved so forceful in the face of lower DIVX prices if consumers did not have to accept the delay and inconvenience inherent in the DIVX dial-up rights authorization every time they wished to play a disc.

113. The necessity of communication with a remote server inevitably increases users' exposure to security risks beyond those that exist in self-contained local authorization mechanisms. In a once-controversial incident that has been all but eclipsed by the Sony BMG "rootkit DRM" fiasco, discussed *supra* notes 50–51 and accompanying text, the company Overpeer, which had been retained by members of the recording industry to upload "spoofed" media files to peer-to-peer ("P2P") networks, uploaded harmful files that relied on a flaw in Microsoft Windows' built-in DRM system to infect P2P users' computers with spyware and adware. Microsoft's DRM system was designed to communicate with a remote server specified in the media file to request license information and terms, but the DRM system included no built-in mechanism to ensure that what the server had transmitted was actually the terms of a license rather than some other type of software. When a user attempted to play one of Overpeer's infected files, the Windows DRM system dutifully contacted a server specified in the file, which then proceeded to swamp the user's system with dozens of pop-up windows and tried surreptitiously to download spyware programs in the background. *See* Andrew Brandt & Eric Dahl, *Risk Your PC's Health for a Song?*, PC WORLD, Dec. 29, 2004, http://www.pcworld.com/article/id,119016/article.html.

Real-world examples of consumer-level DRM systems relying on remote authorization are few.[114] The now-obsolete DIVX video disc technology, an early competitor of DVD discs, was one such system. DIVX disc players, unlike contemporary DVD players, needed to be connected to a telephone line in order to function.[115] When a user attempted to play a DIVX disc, the player dialed a remote server to obtain authorization for the playback.[116] The user could not view the content on the disc until the player had secured the required authorization (and, if necessary, until the user's credit card had been charged for any specified access fee).[117] Unlike the situation with the CSS DRM mechanism employed on DVD discs, mere possession of a disc and a player was ordinarily insufficient to enable a user to play a DIVX disc.[118]

There have been a few general purpose DRM systems based on remote authorization, although they appear to be less common in practice than DRM mechanisms that make authorization determinations at the local user level. A brief sketch of a few remote authorization-based systems illustrates the range of decisionmaking flexibility that their mechanisms offer for DRM-protected digital content.

The Organization for the Advancement of Structured Information Standards ("OASIS"), an international group, has promulgated specifications for the XML-based eXtensible Access Control Markup Language ("XACML").[119] XACML's distinguishing characteristic is that it "assumes a highly distributed environment in which all policies, attributes, and decisions may be remotely sourced."[120] The XACML specifications define the structure of an XML document, called a "policy," that allows users to submit a "request" for a type of access to content stated in the policy, and specifies a "response" to be returned to the user upon the receipt of such a request.[121] The policy drafter can express a number of conditions and limitations in the pol-

---

114. Systems of this sort might be encountered more frequently where fair use is not an issue, for example, in organizations that need to provide differing levels of access to electronic records. *See, e.g.*, Robert L. Mitchell, *Rights of Passage*, COMPUTERWORLD, July 4, 2005, *available at* http://www.computerworld.com/printthis/2005/0,4814,102891,00.html; Michael Voelker, *Content at Risk*, TRANSFORM, Oct. 2004, http://www.transformmag.com/shared/cp/print_article.jhtml?articleID=47902414.

115. *See* Wikipedia, *DIVX*, http://en.wikipedia.org/wiki/DIVX (as of Nov. 16, 2006, 23:29 GMT).

116. *Id.*

117. *Id.*

118. *See id.*

119. *See* Org. for the Advancement of Structured Info. Standards, OASIS eXtensible Access Control Markup Language (XACML) TC, http://www.oasis-open.org/committees/xacml/charter.php (last visited Nov. 16, 2006).

120. Erickson & Mulligan, *supra* note 102, at 991.

121. *See* Org. for the Advancement of Structured Info. Standards, eXtensible Access Control Markup Language (XACML) Version 2.0: Committee Draft 04, at 9–13 (Dec. 6, 2004), http://docs.oasis-open.org/xacml/access_control-xacml-2_0-core-spec-cd-04.pdf.

icy, any of which can supply the basis for triggering a "deny" response.[122] If, and only if, all the stated conditions in the policy evaluate to "permit," the remote authority returns a "permit" response to the user's request.[123] XACML relies on a remote, server-side program to receive and parse user requests (which are then tested against the terms of the policy with which the authorization program has been supplied) and to return a response to each request.[124]

In another illustration of this type of system, a team of Japanese scientists has proposed an online information brokerage called "Copymart" that is intended to operate as a clearinghouse for authorized digital content.[125] The Copymart system employs its own XML-based language, the Copyright Management Framework ("CMF"), to describe and enforce copyright holders' wishes as to the content they contribute to the system. Copyright holders submit content to Copymart marked up with whatever limitations on use they wish to specify in a CMF-based license. A user seeking to make use of content available on Copymart submits a request to the system's "Copy Market" server. The server then compares the terms of the request with the license information previously supplied by the copyright holder. If the terms of the license require a payment for the requested use, and the user has authorized payment, the electronic "negotiation" over the terms of the license concludes automatically, and the user is permitted to engage in the use.[126] Chinese researchers have made a similar proposal that depends on a coordinated exchange of information between a user's "personal information server" (which may be the user's own

---

122. *See id.*

123. *See id.*

124. *See id.* For a description of XACML's decision logic, including sample policies, requests, and responses, see *id.* at 24–31.

125. *See* Copymart Inst., About Copymart: What is Copymart?, http://www.copymart.jp/cmi/about_e_f.html (last visited Nov. 16, 2006) (English-language home page for the Copymart project).

126. In the interests of clarity and space, I have slightly abridged the full sequence of events involved in a Copymart transaction. Fuller explanations may be found in the Copymart creators' academic papers detailing their system. *See* Masayuki Kumazawa et al., *Representation of Reuse Mechanisms for Digital Work with Multiple Right-Holders*, *in* 2001 SYMPOSIUM ON APPLICATIONS AND THE INTERNET — WORKSHOPS 145, *available at* http://doi.ieeecomputersociety.org/10.1109/SAINTW.2001.998222 (abstract describing academic paper); Masayuki Kumazawa et al., *Relationship Among Copyright Holders for Use and Reuse of Digital Contents*, *in* PROCEEDINGS. OF THE FIFTH ACM CONFERENCE ON DIGITAL LIBRARIES. 254 (2000), *available at* http://doi.acm.org/10.1145/336597.336688 (abstract describing academic paper). As the article titles suggest, one of Copymart's advertised strengths is its description of rights held by multiple parties, as, for example, where a new work is created by combining portions from independently copyrighted pre-existing works. Where a given payment must be parceled out among several copyright holders in proportion to the contribution of their original works to a new whole, a Copymart-like system of automated administration of license negotiations and payment would be particularly valuable. *Cf.* FISHER, *supra* note 4, at 234–36 (describing an arrangement for parceling revenues among multiple creators of derivative works under an alternative compensation system).

computer) and a remote license-administering authority to ascertain whether a requested use of DRM-protected content is permissible.[127]

2. Protections for Fair Use

How might fair uses be protected under a DRM system relying on remote authorization? There are at least some reasons to expect that such systems offer more robust protections for fair use rights than local authorization systems can. The magnitude of the improvement, however, depends heavily upon the characteristics of the particular implementation, and systems relying solely on remote authorization may introduce their own problems as well.

At one extreme, a remotely authorized DRM mechanism may be designed simply to duplicate the "hard-coded" decision logic of a locally administered system. That is, the remote computer that receives a user's request for authorization for a given use may be running software that essentially duplicates, rather than improves upon, the capabilities of a locally authorized DRM system such as CSS. In this situation, the switch from local to remote authorization makes the user no better off — and indeed, may make the user worse off if network latency or other connectivity problems delay receipt of the requested authorization.

Despite this drawback, such a system could represent a potential improvement over a "hard-coded" local authorization mechanism. If permitted uses of digital media are stored on a remote server, it becomes relatively simple to simultaneously adjust the permissions for a wide variety of media products merely by tweaking the stored permissions. Centralizing, rather than distributing, the information on which user access to the underlying content depends provides a way to alter the usage rights of many users and many media products at the same time. Of course, users might not prefer such centralization, because permissions might be modified towards greater restriction. The possibility of a subsequent expansion or improvement in end user rights, however, suffices to distinguish a remotely administered mechanism from local authorization DRM systems.

At the opposite extreme, a remotely authorized DRM mechanism may be designed such that every requested use is individually evaluated and acted upon by a human administrator. Such a design would allow the consideration of the greatest amount of contextual information — indeed, the need to reduce such information to machine-parsable form would be eliminated. On the other hand, the potential for delay resulting from human involvement could prove substantial,

127. *See* Yuzhong Qu et al., *OREL: An Ontology-based Rights Expression Language*, *in* PROC. OF THE THIRTEENTH INT'L WORLD WIDE WEB CONF. (WWW2004): ALTERNATE TRACK PAPERS 324, *available at* http://www.www2004.org/proceedings/docs/2p324.pdf.

and the possible sacrifice of user anonymity might also chill controversial, but lawful, uses.

Between these extremes, one might imagine a system that handled certain requests automatically, while relying on human input for other requests. Such a system would fit most naturally into what I have labeled a combined or hybrid approach, discussion of which will be deferred to the next section.

Remotely authorized DRM mechanisms potentially allow for the consideration of complex contextual information in the process of determining whether to authorize a given use of protected content. The gain from such additional information is a decision that hopefully captures more of the complexity of actual fair use practice and the competing interests that characterize situations in the offline world. This hoped-for improvement in decisionmaking, however, comes at a cost.

First, because the user must communicate with the licensing authority, *anonymous* fair use may become difficult or impossible. The remote permission requirements unavoidably compromise user privacy, which may chill fair uses that would occur if privacy could be preserved.[128] Similarly, the requirement to await the grant or denial of permission from a remote source may inhibit *spontaneous* fair uses,[129] although this may be less detrimental where the grant-or-deny decision is automated and essentially instantaneous.

Perhaps most significantly, the identity of the selected remote licensing authority greatly influences the efficacy of a remotely administered DRM mechanism as a vehicle for preserving fair use rights. When a user submits a request to engage in fair use of DRM-protected content, it matters a great deal who decides whether the request should be granted.

A copyright holder that issues content protected by a remotely administered DRM mechanism may, for example, require all permission requests to be submitted through its own license server. There is reason to doubt, however, whether a copyright holder would authorize requested uses that copyright law would recognize as fair. Because the fair use doctrine permits more uses of content than copyright holders would likely authorize, a system that allows the copyright holder whether to permit or deny given use would sharply curtail fair uses of DRM-protected content. For that reason, proponents of DRM systems that rely on remote authorization have generally maintained that such

128. *See* Mulligan & Burstein, *supra* note 39, at 139 (arguing that "[p]rivacy is crucial to the full exploration of purchased works" and that the lack of online anonymity "repels people from the use of expressive materials").

129. *See* Burk & Cohen, *supra* note 104, at 59–60.

systems should not leave these decisions to the copyright holder alone.[130]

To preserve fair use rights, then, it seems we must rule out the copyright holder as a candidate to serve as the licensing authority in a remotely administered DRM system. But who, then, should operate the system? Commentators have not yet settled on a single answer.

Burk and Cohen have suggested that the government should assume the role of licensing authority.[131] They reason that copyright holders should not be placed in the position of controlling or financially influencing the decisions made by the licensing authority because of their obvious interests in limiting fair uses.[132] Would-be fair users, in turn, might have an incentive to finance the operation of a fair use rights clearinghouse, but are generally assumed to lack the means to do so or to organize effectively on their own behalf.[133] Absent a strong reason to believe that either content owners or users should be placed in the position of establishing a licensing authority to authorize fair uses of copyrighted works, the authors conclude that the government should perform this function.[134] Sound policy considerations might also weigh in favor of a government-operated licensing authority because "the public policies underlying fair use require some guarantees of public accountability and institutional longevity."[135] For that reason, the authors conclude, users should be able to apply to the Library of Congress (or some other governmental body) for permission to make fair uses of DRM-protected content.[136]

Mulligan and Burstein offer an alternative conception. In their view, economic competition among multiple private licensing authorities is most likely to yield the greatest protection for end user rights.[137] Therefore, they recommend that users be permitted to choose any of several licensing authorities when requesting authorization for a de-

---

130. *See id.* at 59 ("[T]here may be a strong incentive for the rights holder to deny access just when the public interest most demands access."); Erickson & Mulligan, *supra* note 102, at 993 (stating that a remotely authorized DRM system "has the advantage of injecting human judgment into the flow and can accommodate uses that might be contrary to the interests of the rights holder/originator, *if the decision maker is an independent third party*") (emphasis added).

131. Burk & Cohen, *supra* note 104, at 66–67.

132. *Id.* at 66 ("Content owners are unlikely to pay voluntarily for an institution that facilitates low cost or free access to their works.").

133. *See id.*

134. *Id.*

135. *Id.*

136. *Id.* at 66–67. This proposal is consistent with other authors' arguments that fair use may be conceptualized as a set of permissions granted by the government that override denials of permissions from copyright holders. *See* Fox & LaMacchia, *supra* note 95, at 63 ("To the extent that fair use rights can be encoded as generalized grants from Congress that always exist in the evaluation space of a DRM system's policy evaluator, they can always be considered when determining whether a particular action is allowed.").

137. Mulligan & Burstein, *supra* note 39, at 152.

sired use.[138] To prevent any one licensing authority from acquiring a dominant position and then being subverted by copyright owners, users should remain free to switch from one licensing authority to another at any time.[139]

Depending on the identity of the licensing authority, a DRM system based on remote authorization may offer users protections for fair use far exceeding those that can be hard-coded into a local authorization mechanism, but at the cost of anonymity and spontaneity. Efforts to redress these shortcomings and preserve the breadth of fair uses protectible under a remote authorization system underlie the last major category of DRM technologies to be considered here.

C. A Hybrid Approach

1. Rights Management Architecture

The strengths of DRM systems designed to complete the authorization process at the local end user level lie in their immediacy of response and their capacity for accommodating anonymous and spontaneous uses of digital works. Their weaknesses lie in the limited protections they can provide for fair use due to the difficulty of reducing complex contextual information to machine-interpretable form. Remote authorization DRM mechanisms, in contrast, can potentially take into account a great deal of such contextual data, and thus can accommodate a far greater range of end user rights, while sacrificing immediacy and user anonymity.

What I have labeled the hybrid approach attempts to use the respective strengths of the local authorization and remote authorization approaches to offset each other's weaknesses. It aims for a synthesis that exceeds, in flexibility and power, the predecessor systems from which it draws. The basic concept is relatively simple: media files protected by a DRM mechanism of this type include built-in permissions governing a range of preauthorized uses. Unlike in a pure local authorization system, however, the hard-coded permissions do not define the totality of possible uses of the protected content. Instead, uses that are not covered by the built-in permissions may be authorized remotely through communication with a licensing authority, as with a remote authorization DRM mechanism. By combining the built-in defaults of local authorization with the case-by-case extensi-

---

138. *Id.* ("It is therefore essential that the REL allow users [to] be able to control the choice of processing system . . . .").

139. *Id.* The harm to be prevented here involves possible strategic behavior on the part of the licensing authorities, competing among themselves in a "race to the bottom" to limit user freedoms in the hope of reward from copyright holders in the form of a designation as a preferred (or required) source for processing user requests.

bility of remote authorization, a hybrid mechanism could solve most of the major weaknesses inherent in earlier DRM designs.

Perhaps due to the greater complexity of a hybrid system, no extant DRM mechanism fits cleanly into this category. Some of the remote authorization systems discussed in the preceding section may shade into hybrid systems at the margin, depending on the particulars of the implementation at issue. An XACML-based DRM system,[140] for example, might in practice amount to a hybrid system if it is designed to forward some, but not all authorization requests to a remote licensing authority. That is to say, although XACML permits authorization decisions to be "remotely sourced,"[141] it does not appear to require remote authorization in every instance. An XACML-based DRM system designed to process certain usage requests internally, without requiring communication with a remote licensing server, would essentially be a hybrid DRM mechanism.

Burk and Cohen offer a view of a hybrid DRM mechanism expressly designed to preserve fair use rights to the greatest extent.[142] The result is a "mixed fair use infrastructure," which consists of two "layers" that implement local and remote authorization components.[143]

At the first layer, Burk and Cohen's mixed fair use infrastructure would mandate the inclusion of "automatic fair use defaults based on customary norms of personal noncommercial use."[144] Because copyright holders might otherwise lack any incentive to include such automatic defaults when issuing their own content in digital form, Burk and Cohen would amend the Copyright Act to condition the enforceability of copyrights in United States works on compliance with the fair use defaults.[145] Recognizing the risk that courts may misconstrue this legislatively mandated floor as a ceiling for fair use, Burk and Cohen's proposed "law would clearly state that the level of copying permitted by the automatic defaults does not define the full extent of permitted fair use."[146] Because rights included in the first layer would be preauthorized without the need to communicate with a remote server to obtain additional authority, users would be free to exercise this encoded subset of fair use defaults anonymously and spontaneously.

At the second layer, the mixed fair use infrastructure would implement a remote authorization DRM mechanism allowing users, upon a proper showing, to obtain from an escrow agent the digital

140. *See supra* notes 119–24 and accompanying text.
141. Erickson & Mulligan, *supra* note 102, at 990.
142. Burk & Cohen, *supra* note 104.
143. *Id.* at 65.
144. *Id.*
145. *Id.*
146. *Id.*

keys necessary to make uses of the protected work beyond the automated defaults.[147] Again, to remedy the problem of copyright holder incentives, Burk and Cohen would condition the statutory protection of DRM against circumvention upon the inclusion of a mechanism for obtaining remote authorization for fair uses.[148] Thus, a copyright holder could decline to provide any means for authorizing fair uses beyond the mandatory defaults, but if it declined to do so, users would be free to circumvent the DRM mechanism for noninfringing purposes without penalty.[149] If the copyright holder did include such a mechanism for obtaining remote authorization, it would be entitled, under Burk and Cohen's proposal, to pursue anti-circumvention complaints against users who engaged in uses that had not been authorized either by the built-in first layer defaults or by a remote licensing authority.[150]

Burk and Cohen's proposal places the U.S. government — specifically, the Library of Congress — in the role of remote licensing authority. They reason that the Library of Congress would be well suited to perform this role both because, among other advantages, it has specialized institutional expertise and because copyright owners could be required to make works available to the Library in unprotected form:

> The Library of Congress's long experience with copyright matters and with the deposit and archival preservation of copyrighted works makes it the ideal candidate to fill the escrow role. In our view, moreover, the deposit requirement that currently applies to published or registered works would require copyright owners to provide the Library of Congress with the unrestricted ability to read, view, or listen to the work and to subject the work to any digital storage and search tools that the Library might develop or acquire. Our proposal offers a means of administering fair use access to these deposited works. Finally, the tradition of strong privacy protection by libraries, including the Library of Congress, makes such an institution best suited to maintaining the privacy of fair users. Funding for the fair use infrastructure could be provided either through general taxation, by a small

147. *Id.* at 65–66.

148. *Id.*

149. *Id.* at 66 ("For such unescrowed works, a 'right to hack' would effectively substitute for access via the escrowed keys."). Presumably, to effectuate such a right, it would also be necessary to amend the DMCA to make the distribution and use of such circumventing tools lawful.

150. *See id.*

> administrative fee levied on copyright owners, or by some combination of the two.[151]

Burk and Cohen's mixed fair use infrastructure contemplates protections that, in the aggregate, potentially allow a greater variety of uses than do more restrictive traditional DRM mechanisms. Burk and Cohen also recognize that acceptance of their system might depend on guaranteed protection of trade secrets in light of the relaxation on allowed uses. To prevent the system from becoming a tool for commercial espionage, Burk and Cohen would exempt any work protected by trade secret law from their system, albeit with the express caveat that "[a] work should not be deemed to contain trade secrets simply because the copyright owner has elected to shroud it with technological protection."[152]

2. Protections for Fair Use

How well would a hybrid DRM system such as Burk and Cohen's protect fair uses of copyrighted works? Burk and Cohen acknowledge that the open-ended character of fair use under United States law makes it particularly difficult to model in machine-executable form, especially when contrasted with the more discrete, specific copyright exceptions traditionally recognized under European law.[153] Even European law, however, includes its share of ill-defined, context-dependent standards that would be challenging to describe in terms amenable to automated execution.[154] Both American and European users, Burk and Cohen believe, would ultimately benefit from the type of system they describe:

> Our proposal will not exactly reproduce the conditions of fair use in traditional media. Although code is malleable, digital media work differently than traditional media in too many ways. Nonetheless, we think that a mixed fair use infrastructure based on both automatic default and key escrow elements would go a long way toward approximating traditional fair use conditions. We note, as well, that de-

---

151. *Id.* at 66–67 (footnotes omitted). Of course, a rights management proposal premised upon a "tradition of strong privacy protection by libraries" must contend with the reality of diminished protections available under Section 215 of the USA PATRIOT Act, 50 U.S.C.A. § 1861 (2006), as well as the present administration's litigation posture that the procedural requirements of the Foreign Intelligence Surveillance Act ("FISA"), 50 U.S.C.A. §§ 1801–1862 (2006), are optional in any event.

152. Burk & Cohen, *supra* note 104, at 67.

153. *Id.* at 70.

154. *Id.* at 70 & n.83; *see also infra* note 285 and accompanying text.

> velopment of a mixed infrastructure for digital fair use might lead to recognition of "new" fair uses never needed for works in nondigital media — for example, a right to access a work for certain purposes after expiration of a time-limited subscription agreement. Thus, our proposal would enable the continued evolution of fair use practices and norms.[155]

Hybrid DRM mechanisms promise to better approximate fair use than either local or remote authorization alone could. Local authorization mechanisms are desirable insofar as they allow anonymous, spontaneous uses of the protected content, but they are heavily dependent upon the foresight of the DRM developer to anticipate particular fair uses, and may be unable to accommodate the types of contextual detail underlying legal decisions on fair use. Remote authorization mechanisms are desirable insofar as they allow users to acquire necessary permissions separately from the protected content and may reintroduce an element of human decisionmaking into the authorization process, but the improvement sacrifices user anonymity and may also inhibit spontaneity. Alternatively, a combination of local and remote authorization — using the strengths of each approach to offset the weaknesses of the other — may create a tolerably close approximation of fair use rights as they exist in the offline world. A hybrid DRM mechanism potentially allows a content-rich, context-sensitive environment for fair uses of DRM-protected digital works.

D. Lingering Problems

Despite the improvements available in a hybrid DRM mechanism over systems relying wholly upon local or remote authorization, such a system might fail to duplicate the conditions of fair use as closely as its proponents contend. Although a hybrid DRM mechanism has certain advantages over less technologically sophisticated alternatives, it relies on inherent design features and technological assumptions that may prevent it from fully implementing fair use rights.

1. The Requirement of Permission

One feature common to local authorization, remote authorization, and hybrid DRM systems is the requirement that the user obtain permission for any desired use. The various systems differ as to how that

---

155. Burk & Cohen, *supra* note 104, at 70. I share Burk and Cohen's goal of "enabl[ing] the continued evolution of fair use practices and norms" in the digital domain. *See supra* note 20. As discussed *infra* Part III.D, however, Burk and Cohen's design seems to me poorly suited to enable such an evolution.

permission is described, sought, and granted, but the requirement of permission is a constant. Permission becomes the *sine qua non* of access; if the request for authorization is denied, the DRM mechanism refuses to permit the user to engage in the requested use.

Thus, the "deny by default" regime criticized in the discussion of local authorization DRM mechanisms continues,[156] in only slightly modified form, in remote authorization and hybrid DRM systems. Each establishes a procedure — a list of steps that must be followed — to effectuate a user's wish to employ the DRM-protected content in some fashion. Each of the required steps must be carried out, and the authorization must be communicated in the fashion the DRM mechanism is programmed to recognize, or else the content remains inaccessible. The requirement of permission, however varied in its particulars from one design to the next, always bars the requested use of the work unless and until its conditions are satisfied. The door remains locked until someone empowered to do so gives the user the key.

One might justifiably question whether it is correct to attach the label "fair use" to uses that are authorized by the copyright holder or its designee. In the offline domain, fair use and permission are, if not antagonistic, at least mutually exclusive. The copyright owner's permission eliminates the need to resort to the fair use doctrine. Conversely, the fair use doctrine protects fair uses not only where the copyright owner's permission was never sought, but also where permission has been sought and refused. Can any DRM system that makes authorization by an outside party the *sine qua non* of access truly protect what the law would recognize to be fair uses?

A possible answer to this objection has already been hinted at in the prior discussion of granting the power to authorize fair uses of DRM-protected works to parties other than the copyright holder.[157] If we conceptualize fair uses as a set of permissions granted by the government that override any wishes of the copyright owner to the contrary,[158] and we effectuate that conception by empowering a government agency to approve requested fair uses without the copyright owner's involvement,[159] could such a system not protect at least some uses that the law would undoubtedly recognize as fair?

Granting a disinterested party, such as the government, the authority to authorize requested fair uses of DRM-protected digital content certainly eliminates one of the possible outcomes distinguishing fair use in the digital domain from fair use in the offline world:

156. *See generally supra* note 100 and accompanying text (providing an earlier critique of the "deny by default" regime).

157. *See supra* notes 130–39 and accompanying text.

158. *See* Fox & LaMacchia, *supra* note 95, at 63.

159. *See* Burk & Cohen, *supra* note 104, at 66–67.

namely, the risk that a copyright holder's disapproval will always prevent a desired use. To match conditions in the offline world, a copyright holder must be legally (and technologically) powerless to prevent fair uses in the digital domain. Giving the final say to an independent licensing authority, to the extent that it prevents such a copyright holder veto, is a way to at least partly mimic the characteristics of the offline world in a DRM-protected digital realm.

Yet this answer does not address all of the objections to a permission-based DRM mechanism. In the world of offline media, a user seeking to engage in a fair use of a copyrighted work does not need advance permission from *anyone*. External decisionmakers become involved, if at all, only *ex post*. As a matter of process, the exercise of fair use rights in the offline world initially depends solely on the user's unilateral act. The user's conduct may, to the extent that it becomes known, be scrutinized after the fact for its compliance with the law, but nobody (including the copyright holder and the government) is entitled to advance notice or an opportunity to prevent the use from occurring.[160] Any DRM mechanism that leaves the ultimate decision whether a given fair use can occur in the hands of parties other than users themselves, accordingly, departs from the process of fair use as it occurs in the offline domain.

2. Permission and Privacy

A related objection concerns the issue of user privacy in DRM mechanisms that require approval from an outside licensing authority. Although a hybrid system combining local and remote authorization mechanisms may supply users with some privacy protection, this protection may be more theoretical than real once we consider *which* requested uses will most likely require the user to seek outside authorization.

In a remote authorization DRM mechanism, every requested use of protected digital content must be authorized by some remote licensing authority, and concerns about user privacy apply with full force. Hybrid DRM mechanisms partly assuage these privacy concerns by "pre-approving" a subset of recognized fair uses. That is to say, some types of fair uses are hard-coded into the content and may be exercised without requesting external authorization (and therefore without disclosing the desired use to the licensing authority).

Even in such a hybrid system, however, the uses most likely to need external authorization are those most difficult to foresee and reduce to code. These, in turn, may be those uses that are "closest to the

160. *See* Erickson & Mulligan, *supra* note 102, at 992–93 (discussing differing incentives provided in a system in which policy enforcement occurs before, rather than after, a user engages in a putative fair use of copyrighted content).

line," in which the various contextual factors play the strongest role. Quoting excerpts from the core of a controversial work, possibly thereby dampening demand for the work,[161] is one example of a use that might fall sufficiently close to the line of fairness to require the careful balancing of factors that can be achieved, if at all, only by an external decisionmaker.

It is precisely in such circumstances, however, that concerns about preserving user privacy are most prevalent. Thus, although hybrid DRM systems purportedly improve on pure remote authorization systems by restoring a domain for anonymous fair uses, the uses that will continue to require outside authorization are precisely those in which concerns about eroding user privacy are strongest.[162]

The baseline of fair use in the offline world accommodates user privacy — typical fair uses occur essentially anonymously. Remote authorization DRM mechanisms ignore user anonymity, and hybrid systems may provide it only in those circumstances in which it is of lesser concern. In departing from the ideal of anonymous fair use, even hybrid DRM mechanisms aimed at providing an avenue for users to pursue fair uses fail to capture crucial characteristics of fair use in the offline world.

IV. STRENGTHENING PROTECTIONS FOR FAIR USE RIGHTS IN DRM

Although many observers have recognized the need for DRM mechanisms to include copyright exceptions such as fair use, both existing and proposed DRM systems poorly implement such exceptions. While some have concluded that working to develop technological protections for fair use is a futile endeavor,[163] I believe it may be worthwhile.

The flaw in the conclusion that DRM cannot accommodate fair use is an unduly hasty inductive leap from the specific (the impossibility of modeling the substance of fair use law in machine-administrable form) to the general (the supposed impossibility of protecting fair use at all in DRM systems). The foreclosure of one avenue for protecting fair use, however, does not imply that all avenues are likewise foreclosed, but only that design principles other than the creation of a perfect "judge on a chip" must be explored.[164] Shifting

161. *Cf.* Harper & Row Publishers, Inc. v. Nation Enters., 471 U.S. 539, 569 (1985) (holding that quoting a 300-word excerpt from the core of an unpublished work was not fair use).

162. *See infra* Part IV.B.2.

163. *See, e.g.*, Dan L. Burk, *Legal and Technical Standards in Digital Rights Management Technology*, 74 FORDHAM L. REV. 537, 550 (2005).

164. Stefan Bechtold has chided DRM critics for paying insufficient attention to the evolution of "dynamic DRM" tools that may protect the rights of both copyright holders and

the focus to the protection of the *process* of fair use — the use of copyrighted content by individuals based merely on an exercise of their own volition, subject to scrutiny, if at all, only after the fact — represents one such alternative.

A. Design Principles

The literature on technological protections for fair use provides a number of thoughtful suggestions concerning how best to implement copyright exceptions.

1. Allowing Users to "Challenge the Code"

Erickson and Mulligan recognize the possibility that a DRM mechanism might accept some input from end users in the authorization process.[165] Their discussion, however, is comparatively cursory, and seems to be offered more as a remark in passing than as a substantial proposal for future reform:

> In this conventional view of the trusted system, the *code* becomes the ultimate arbiter; there are typically no technical provisions that allow the individual to disagree with the system's determination, regardless of whether the user may *legally* be in the right . . . .
>
> Policy-enforcement systems that accommodate variable use requests from individuals could provide those users with a limited ability to "challenge the code," in the sense that they could request authorizations for controlled actions for reasons other than purchase. In extreme cases, these requests might even deliver to individuals technical capabilities not

---

users alike. *See* Bechtold, *supra* note 6, at 602–05; *see also id.* at 602 ("Nothing in the 'nature' of DRM requires that DRM be only used for restricting access to protected content or suppressing fair use privileges."), 604 (describing ongoing research in rights expression languages "able to manage transformative uses, overlapping innovation, and the creation of derivative works in a fine-grained way"). Dan Burk believes Bechtold's "assessment of future DRM is unduly rosy" in view of "the inability of DRM to accommodate legal standards." Burk, *supra* note 163, at 550 n.60. Bechtold, it seems to me, has the better of this argument. Bechtold's argument builds upon research aimed at expanding the technological capabilities of parties other than the original content holder to assert their own rights over the protected content. What makes that research promising is that it does not seek to "accommodate legal standards" in DRM, but instead aims to create DRM technologies that do not make the vagueness of governing legal standards outcome-determinative. The impossibility of creating a "judge on a chip," programmed with full knowledge of the substantive law of fair use, simply means that effective protections for fair use rights in DRM must take a different form — a prospect that Bechtold recognizes but Burk ignores.

165. Erickson & Mulligan, *supra* note 102, at 995.

> previously installed in content-handling components.[166]

Having raised the prospect that an external authority's decision to deny permission might not be the final word on the question, Erickson and Mulligan do not develop the idea further or explore how it might be implemented in practice. Nevertheless, even the brief excerpt quoted above includes a number of important observations that may supply useful guidance when attempting to design a DRM mechanism that incorporates strong protections for fair use rights.

First, Erickson and Mulligan hint at a DRM mechanism that, unlike virtually all the examples collected in Part III, would foster an ongoing dialogue between users and administrators of the DRM system, along with possible input from outside parties, rather than a one-shot request-and-response system for obtaining permissions to use digital works.[167] Erickson and Mulligan raise the possibility that a denial of a requested use (or even a grant conditioned upon compliance with requirements a user finds too onerous) could be subjected to further review inside or outside the DRM system.[168] Although the authors do not discuss the type of outside review that would be appropriate or how it could be effectuated, their proposal nevertheless hints at a possible opening-up of DRM mechanisms that are ordinarily considered closed and self-contained.

Second, the excerpt quoted above recognizes a potential consequence of increased user empowerment for the design of DRM software. The software that implements the DRM system may need to be modular and extensible in design, accommodating components that permit unrestricted playback and duplication where such uses have been deemed fair. Indeed, because in some circumstances fair use permits duplication of an entire work,[169] software may need to be engineered so as to allow unfettered duplication in those circumstances. As discussed in Part V below, this requirement may have substantial implications for the political feasibility of the adoption of any DRM mechanism engineered to accommodate fair use rights.

---

166. *Id.* at 994–95.

167. *Id.* at 995.

168. *Id.*

169. *See, e.g.*, Sony Corp. v. Universal City Studios, Inc., 464 U.S. 417, 456 (1984) (home taping of complete television broadcasts for purpose of "time shifting" held fair use). Entertainment industry attorneys recently conceded before the Supreme Court that copying a complete song from an audio CD to an MP3 player was noninfringing. Transcript of Oral Argument at 12, Metro-Goldwyn-Mayer Studios Inc. v. Grokster, Ltd., 545 U.S. 913 (2005) (No. 04-480); *accord* Recording Industry Ass'n of Am. v. Diamond Multimedia Sys., Inc., 180 F.3d 1072, 1079 (9th Cir. 1999) (describing copying MP3 files from one's own CDs to portable digital music player as "paradigmatic noncommercial personal use"). *But cf.* FISHER, *supra* note 4, at 99–100, 117–19 (discussing court findings in earlier cases that "ripping" one's own audio CDs was not fair use).

2. Revising XML-Based Rights Expression Languages

Another paper co-authored by Professor Mulligan imagines what technological alterations of existing DRM designs would be necessary to improve protections for fair use.[170] Mulligan and Burstein aim to tie their discussion closely to current-generation DRM technologies by focusing their attention on the XrML language.[171] To improve protections for fair use, Mulligan and Burstein suggest changing current RELs, including XrML itself, to make it easier to express context-dependent policies such as fair use, and adding a new messaging protocol to XrML that would allow end users to assert rights over content in their possession.[172]

Mulligan and Burstein begin by highlighting several respects in which XrML and other current-generation RELs fail to capture limitations on copyright holders' exclusive rights under federal copyright law. Although the Copyright Act includes many limitations on copyright holders' exclusive rights, "[m]achine-readable rules that control access to digital works could inhibit, restrict, or altogether prevent many legally authorized uses."[173] The obvious risk is that, particularly for content offered only in DRM-protected digital form, "these machine-readable rule sets . . . could supplant copyright law."[174]

Beyond the express copyright exceptions, Mulligan and Burstein also note that "real space norms," not expressly stated in the statutory text, "have developed around the use of copyrighted works."[175] For example, "the private use of copyrighted materials" remains "essentially unregulated."[176] Where such uses are at issue, copyright holders traditionally have not been thought to enjoy any right "to require readers, viewers, or listeners to seek authorization before using a work privately."[177] This historical practice, while not expressly protected by the Copyright Act, nevertheless underlies an expectation of privacy in personal uses of copyrighted works. The authors note that the express copyright exceptions and the social norm of private use establish an important baseline for the use of copyrighted works which most DRM mechanisms do not meet:

> The evolution of fair use depends on, and the exercise of exceptions to copyright presupposes that, *users may determine for themselves whether to seek*

170. Mulligan & Burstein, *supra* note 39.
171. *Id.* at 138 n.1; *see also supra* notes 92–93 and accompanying text.
172. Mulligan & Burstein, *supra* note 39, at 138.
173. *Id.* at 138.
174. *Id.*
175. *Id.* at 139.
176. *Id.*
177. *Id.*

> *"permission"* for a given use. The Copyright Act provides a framework that allows "rights" to flow from several sources — the owner of the object (or copyright holder), a third party (including the government), and the user.[178]

Most current DRM technologies invert this presupposition: DRM allows the copyright holder to compel the user to seek permission for any requested use, and to deny the use entirely if the user's permission request fails (assuming that the DRM system is engineered to accommodate such requests at all). As Mulligan and Burstein write, "common RELs take the exclusive rights of copyright as an unqualified baseline and then provide the means for rights holders to make the work available under issuer-defined access models."[179]

The authors suggest several approaches for rectifying the shortcomings of current DRM systems. First, they would extend the vocabulary of rights that can be described in XrML, allowing exceptions to copyright holders' exclusive rights to be described. Put another way, Mulligan and Burstein aim to allow users' rights, not merely copyright holders' rights, to be described in XrML in machine-interpretable form, so that "[t]he user's claim of right would provide the essential information for a usage-rights issuing agency to give the user the technical capability to use the work in a particular way."[180]

This suggested extension of the vocabulary in which rights are expressed suggests a second, more far-reaching, change. Like most RELs, XrML assumes "a top-down, unidirectional flow of rights."[181] This "assumption of a one-way expression of rights," however, has produced recognizable "deficiencies in the RELs that are currently available."[182] To remedy these deficiencies, Mulligan and Burstein suggest replacing XrML's messaging layer with a new Rights Messaging Protocol ("RMP") that would allow "bi-directional exchanges" of rights information.[183] By allowing the assertion of rights in a bottom-up fashion, the authors' proposed new RMP would effectuate users' practical ability to use the copyright exceptions enacted for their benefit.[184]

---

178. *Id.* (emphasis added).
179. *Id.*
180. *Id.* at 141.
181. *Id.* at 140.
182. *Id.* at 141.
183. *Id.*
184. As Mulligan and Berstein explain:

> At a minimum, recipients of works must have the ability to assert their rights as recognized under copyright law, and have these assertions reflected in their ability to use the work. Extending an REL to support a broader range of statements that reflect current law is, however, insufficient. The [RMP] layer

Mulligan and Burstein's proposal displays remarkable sensitivity to concerns about user anonymity and privacy. Although Mulligan and Burstein would provide every user with the tools necessary to assert fair use rights over DRM-protected digital content, they would not mandate an express assertion of rights in every instance. Their proposal, instead, contemplates that DRM systems should allow a wider range of default positions and move away from the "closed-universe" approach in which every use not expressly authorized is deemed to be wrongful. One of the major problems of existing RELs such as XrML is that they do not make fair use a default right of the license.[185] Their proposal would remedy this shortcoming by substituting a series of default rights, each geared towards a particular medium, in place of XrML's "one-size-fits-all" approach, which is purposefully agnostic as to the type of media being protected.[186] Different types of media would be subject to different defaults, not all of which would require users to make an express assertion of rights before being able to use the work in one of the specified ways.[187] Mulligan and Burstein provide an example using specific proposed tags from XrML:

> . . . if a `Work` is a `MusicalAlbum`, the default interpretation of the `License` must be that the `Principal` — the music critic, who bought the album — must be able to play the album without restriction, and to copy arbitrary parts of the album. This suggests that a concrete `Work` would impose certain default `Rights`, which would be granted by a given kind of concrete `Work`. In the case of a `MusicalAlbum`, this would include `"Play," "Rewind," "Seek,"` and `"Excerpt"` or `"Copy" Rights`. Similar default `Rights` can be specified for different kinds of `Works`.[188]

In addition, Mulligan and Burstein would mandate a series of protections to ensure that their proposed DRM system does not become a tool for user surveillance by copyright owners. Again, the authors take offline user norms that have developed under federal copyright law as their baseline. Those norms include robust protections for user privacy, partly for the simple reason that most fair uses of non-DRM-

---

> must also be extended to accommodate both the downstream and upstream assertion of rights.

Id.

185. *See id.* at 145.

186. *See id.* at 146.

187. *Id.*

188. *Id.* For clarity, I have kept their original typeface to distinguish the XrML tags.

protected content are undetectable and effectively anonymous.[189] To reflect the realities of the offline world, the DRM "processing system should make no inquiry into the extent or frequency with which the user seeks to exercise the rights."[190] To minimize the risk that copyright owners will compel users to bargain (and pay) for rights that the fair use doctrine makes freely available, the authors' DRM system would be designed not to record the types of personally identifying information on which such a bargaining approach would depend.[191]

3. LicenseScript

A group of academic and industry authors from the Netherlands has suggested a novel approach that would implement a number of Mulligan and Burstein's suggestions. Rather than seeking to improve the recognition of fair use and other copyright limitations in existing RELs such as XrML, this group has instead designed its own computer language for DRM systems. Their language, LicenseScript,[192] is based on the high-level, general-purpose programming language Prolog.[193]

LicenseScript aims to overcome several failings of XML-based languages like XrML. First, XrML can be an extremely verbose means of expressing rights, particularly when attempting to describe the complex conditional rights structures that are common in real-world applications.[194] As the designers of LicenseScript put it,

189. *Id.*

190. *Id.* at 147.

191. *See id.* at 146–48. This design feature is particularly desirable insofar as it follows Professor Cohen's admonition against collecting user-identifying information except where such information is required for functional purposes. *See infra* note 228 and accompanying text.

192. *See* Cheun Ngen Chong et al., LicenseScript: A Novel Digital Rights Language and its Semantics, http://purl.org/utwente/fid/1152 (2003) [hereinafter Cheun et al., LicenseScript].

193. Prolog is frequently deployed in artificial intelligence applications and is generally known for its comparatively simple and lucid syntax. *See generally* Wikipedia, *Prolog*, http://en.wikipedia.org/wiki/Prolog (as of Nov. 17, 2006, 00:24 GMT).

194. *See, e.g.*, XrML Example Use Cases, *supra* note 102, at 8–12, 31–40. The authors' LicenseScript language enjoys a relatively compact syntax. Indeed, to drive home the strength, flexibility, and concision of their language, some of the same authors produced a much longer paper in which they rewrote nearly all of the basic usage examples supplied with XrML and the Open Digital Rights Language ("ODRL") in LicenseScript. In general, the LicenseScript examples are substantially shorter than their counterparts in the XML-based RELs, and take full advantage of LicenseScript's license-rewriting capabilities. *See* Cheun Ngen Chong et al., *Comparing Logic-Based and XML-Based Rights Expression Languages*, *in* ON THE MOVE TO MEANINGFUL INTERNET SYSTEMS 2003: OTM 2003 WORKSHOPS, LNCS 2889, at 779 (Robert Meersman & Zahir Tari eds., 2003). An even lengthier version of the article, including appendices containing many more examples of XrML code and the corresponding implementation in LicenseScript, is available on the authors' web site. *See* Cheun Ngen Chong et al., Comparing Logic-Based and XML-Based Rights Expression Languages, http://purl.org/utwente/fid/1138 (last visited Nov. 17, 2006).

XrML's "syntax is complicated and obscure when the conditions of use become complex."[195] Second, XrML has been criticized as overly dependent on human inferences and interpretations to give content to many of the terms used in license grants (such as "play," in the context of an entertainment work).[196] Finally, because of their limited capability to accommodate contextual data, XML-based RELs "cannot express many useful copyright laws."[197]

A technical description of the syntax and operation of LicenseScript lies beyond the scope of this Article. For purposes of the present inquiry, however, the most provocative work by the authors of LicenseScript is their essay, *Approximating Fair Use in LicenseScript*.[198] In this work, the authors examine whether LicenseScript can accommodate provisions reasonably analogous to fair use law as it exists in the United States. Their work is particularly interesting in that it draws upon both scientific and legal scholarship as inspiration for its novel DRM proposal. Thus, for instance, the authors approvingly note Mulligan and Burstein's summary of the limitations of XML-based RELs in accommodating fair uses.[199] The authors next ask whether LicenseScript can succeed where XML-based RELs have failed. Their answer is a qualified "yes."

The authors propose a two-part approach to approximating fair use rights in LicenseScript: "(1) *Rights assertion*: to allow the user [to] assert new fair use-compliant rights in addition to the rights dictated by the license; and (2) *Audit logging*: to keep a record of the rights asserted by the user and [to keep track of] the copies of the licenses created."[200] This two-part approach, in the authors' view, evenhandedly accommodates the interests of both digital content users and copyright holders: "on one hand, the users can freely exercise their statutory rights; on the other hand, the copyright owner can track the source of possible copyright infringement."[201] Allowing users "to assert new rights contributes to fair use because [they] can express their rights according to their will, in addition to the rights granted by the copyright owner."[202]

---

195. Cheun et al., LicenseScript, *supra* note 192, at 1.

196. In XML-based RELs, "the meaning of licenses relies heavily on . . . human interpretation." *Id.*

197. *Id.* (citation omitted).

198. Cheun Ngen Chong et al., *Approximating Fair Use in LicenseScript*, *in* DIGITAL LIBRARIES: TECHNOLOGY AND MANAGEMENT OF INDIGENOUS KNOWLEDGE FOR GLOBAL ACCESS, PROCEEDINGS OF THE 6TH INTERNATIONAL CONFERENCE ON ASIAN DIGITAL LIBRARIES, LNCS 2911, at 432 (Tengku M.T. Sembok et al. eds., 2003), *available at* http://purl.org/utwente/fid/1136 [hereinafter Cheun et al., *Approximating Fair Use*].

199. *Id.* at 433 (citing Mulligan & Burstein, *supra* note 39).

200. *Id.* (citation omitted).

201. *Id.* at 434.

202. *Id.*

Under this proposal, digital content protected by a DRM mechanism implemented in LicenseScript would convey to the user permissions typical of DRM mechanisms in general, such as the rights to play back, duplicate, excerpt, or print a work. In addition, the licensor would encode a new right — "assert" — in the clauses of the license and the accompanying playback rules. In the authors' examples, a user would be required to supply four pieces of information to exercise this new "assert" right: (1) the user's identity, (2) the right asserted, (3) the date of the assertion, and (4) the purpose for which the content is sought to be used.[203] The "purpose" item must be chosen from a list of six possibilities encoded with the license: criticism, comment, news reporting, education, scholarship, or research.[204]

The LicenseScript proposal includes two mechanisms designed to protect copyright holders against abuse of users' powers to assert new rights over the protected content. The first is, essentially, a conscious abandonment of user privacy: every assertion of a fair use right would be recorded in the license along with the user's identity, the date, and the proffered reason for the use. This creates an audit trail of asserted fair uses that the copyright holder may ultimately be able to inspect. The possible risk of future discovery, the authors assume, will give users an adequate incentive to confine their assertion of new rights to circumstances that truly constitute fair uses of the protected work.[205]

The second mechanism protecting copyright holders is subtler, but likely more directly effective, than the power to police asserted fair uses through the audit trail. Although the new "assert" right empowers users to alter the supplied license clauses to give themselves new rights not included in the original license, *the asserted rights must themselves be reflected in the license rules*. A user cannot effectively assert a right to print the document, for example, if the content provider has not programmed the license rules to recognize "printing" as a right. The ultimate choice of which capabilities will be recognized and effectuated thus remains with the original licensor.[206]

---

203. *Id.* at 435.

204. *Id.* at 439.

205. LicenseScript's authors are, perhaps purposefully, vague on the possible mechanisms by which copyright holders could monitor the uses of protected works. The license rules as given in their examples do not, for example, include any provision for automatically forwarding to the original licensor a copy of any modified licenses created as a result of users' assertions of new rights. The audit trail of users' assertions of fair use rights will travel with the accompanying content, however, such that if the content is subsequently sold or transferred from one user to another, the audit trail written in the license bindings will remain intact and readable. *See id.* at 440–41. This feature of the authors' approach, of course, potentially leaves the history of user rights assertions subject to possible inspection not only by the copyright holder, but also by other users.

206. *See id.* at 442 ("Our approach . . . allows user[s] to freely express their rights. At the same time, the copyright owner may control the user's fair use actions to the extent confined by the rules.").

This latter flaw suggests more generally that LicenseScript, despite its undeniable promise, ultimately represents a failed attempt to model adequate protections for fair use in DRM. To be sure, LicenseScript improves in some respects upon the protections for fair use that exist under Burk and Cohen's proposed mixed fair use infrastructure[207] insofar as LicenseScript allows users to assert rights not granted in the original license and does not require asserted fair uses to be disclosed in advance for approval by the license issuer. It is also strongly to LicenseScript's credit that it does not allow the copyright holder to capture an additional royalty as a condition for allowing a user to engage in a fair use of the protected work. Nevertheless, lingering flaws in LicenseScript's design, at least as described by its authors, suggest that it may prove inadequate for protecting fair use rights in DRM.

LicenseScript's primary failing is that, contrary to its stated aims, it actually falls well short of truly permitting users to assert new rights in content they have purchased. A closer look at what LicenseScript actually requires reveals that content owners retain strong control over the rights that may be recognized and asserted by users within the system.

I previously criticized Burk and Cohen's proposed mixed fair use infrastructure for implicitly resting on the same "deny by default" assumption that makes local and remote authorization mechanisms poor protectors of fair use.[208] The solution to that design problem has been well stated by Mulligan and Burstein:[209] DRM designers must grant parties other than the copyright holder, including users themselves, a voice in the authorization mechanism, which must be designed not to leave the copyright holder with the final say.[210] Although LicenseScript's authors cite Mulligan and Burstein's research,[211] they do not heed its insights. LicenseScript, despite its innovations, continues to exhibit the same "deny by default" design that has made prior DRM implementations poor protectors of fair use rights.

LicenseScript's authors repeatedly conceptualize the assertion of new rights as something the copyright holder may permit, at its election, under circumstances of its choosing. Even their attempt to model fair use rights in LicenseScript leaves critical matters under the express control of the original license issuer. The issuer specifies, in its LicenseScript rules, which rights a user may assert — that is to say, which types of access the player application or other access mecha-

207. *See generally supra* Part III.C.
208. *See supra* Part III.D.1.
209. *See* Mulligan & Burstein, *supra* note 39.
210. *See supra* Part IV.A.2.
211. *See supra* note 199 and accompanying text.

nism will recognize as the proper object of an "assert" command.[212] The license issuer is further allowed to delimit the permissible purposes for which a user may assert a right to make use of the protected content.[213] Tellingly, the purposes enumerated in the authors' article omit any reference to certain types of fair use (such as parody) that are clearly established under copyright law but to which copyright holders are very likely to object.[214] Although this may be a simple oversight on the authors' part, and not fatal to the creation of parodies of works protected by a LicenseScript-based DRM mechanism,[215] the omission of a category of permissions that a copyright holder would be disinclined to grant nevertheless highlights the inherent limitations of any system that places so much control in the hands of the copyright holder.

LicenseScript is also subject to a strong privacy objection regarding its audit trail. Every time a user asserts a fair use right over a protected work, LicenseScript records several details of the assertion (including the user's identity) in the license bindings, which thereafter remain attached to the content even if it is transferred to another user or returned to the copyright holder. There are at least two possible objections to this approach.

First, even if we assume that copyright holders need the information collected in the LicenseScript audit trail to police users' rights assertions for possible abuse, that hardly justifies sharing the same information with fellow users. By encoding the details of any asserted fair use in the license bindings, however, LicenseScript assures that a record of the asserted use will follow the content wherever it goes. This needless exposure of one user's identifying data to others could have been avoided if, for example, LicenseScript transmitted records of rights assertions directly to the copyright holder (or, preferably, to a

212. *See* Cheun et al., *Approximating Fair Use*, *supra* note 198, at 439–40.

213. *Id.* at 439.

214. *Cf. supra* notes 33–34 and accompanying text.

215. A user could, for example, simply label its use with one of the other categories enumerated in the article, such as criticism or comment. *See supra* note 204 and accompanying text. This would, in turn, reduce the precision of the license's audit trail, but unless the content owner ultimately viewed both the license audit trail and the resulting parody, it would be none the wiser.

The idea of recording false information in the LicenseScript audit trail where necessary to conform the user's assertion of fair use rights to the more limited subset of permissible uses is analogous to the so-called "owner override" proposal. Advanced by the Electronic Frontier Foundation ("EFF"), the "owner override" proposal would permit users to supply false or misleading information to purveyors of "trusted computing" systems where necessary to maintain the level of control users have customarily exercised over their own PCs. *See* Seth Schoen, Trusted Computing: Promise and Risk, 12 (2003), http://www.eff.org/Infrastructure/trusted_computing/20031001_tc.pdf. Although owner override is too blunt a tool to substitute effectively for a DRM mechanism engineered to preserve fair use rights, it is difficult to quarrel with the EFF's conclusion that such measures can be appropriate where unilateral action by outside parties would otherwise strip users' control over computing devices they have purchased.

disinterested intermediary) rather than writing them into the license bindings.

Second, LicenseScript's rights assertion mechanism potentially supplies copyright holders with a great deal of information about fair users, including their identity, the date and type of use, and the claimed justification, at a time when the copyright holder has no colorable entitlement to know that information. LicenseScript obliges innocent users operating within the confines of the fair use doctrine to surrender their anonymity as a condition of exercising their statutory rights. In this respect, LicenseScript disadvantages users of digital content; fair users in the offline world may remain effectively anonymous unless and until a copyright holder acquires reason to investigate.

B. Designing DRM to Protect Fair Use

Although prevalent DRM technologies currently do a poor job of protecting user rights to engage in fair uses of the underlying works, some commentators have suggested that these rights may be adequately protected by modifying the DRM system to allow user participation in the authorization process.[216] LicenseScript, despite its shortcomings, demonstrates that a system engineered to provide such user participation is technologically feasible.[217] It may be possible to devise a DRM mechanism that adequately protects fair use and user privacy without requiring copyright holders to relinquish the legitimate protections against mass infringement. The discussion that follows aims to provide one possible blueprint for such a system. The basic principles of the design derive from LicenseScript's model, with modifications aimed at overcoming some of its shortcomings.

1. Asserting User Rights and Audit Logging

LicenseScript's designers correctly perceived that fair uses ordinarily rest upon the exercise of a user's volition alone. Any DRM system designed to preserve the range of fair uses that exist in the offline world must, accordingly, leave some space in which users may exercise their fair use rights without needing to petition any external authority for permission. LicenseScript aims to provide such a space, but subordinates user rights to the demands of copyright-holder control. If a DRM system is to approximate the freedoms users enjoy in the offline world, it must include a mechanism for users to unilaterally assert fair use rights, without obtaining advance permission from any out-

216. *See supra* Parts IV.A.1, IV.A.2.
217. *See supra* Part IV.A.3.

side authority. This design principle suggests some alterations to the LicenseScript approach.

First, a DRM system must empower users to assert fair use rights irrespective of the contrary wishes of the copyright holder or any third party. A design, such as LicenseScript or Burk and Cohen's mixed fair use infrastructure,[218] which leaves an outside authority with the final say whether to allow users to exercise their rights, is ultimately incompatible with a mandate to preserve fair use. Therefore, one key component of any DRM system engineered for fair use will be the removal of copyright holders' or other outside parties' ability to prevent users from partaking in putatively fair uses of the protected content. This principle has consequences both for the law and for the design of DRM systems.[219] It suffices here to note that those components of the LicenseScript design that require the original license issuer to authorize the permitted usage before a user becomes empowered to engage in a fair use must be discarded.

Second, a DRM system should not allow the copyright holder to determine which fair uses will be permitted or which purposes the DRM mechanism will recognize as legitimate. What copyright holders cannot deny wholesale, they should not be able to deny piecemeal. A distinct failing of LicenseScript is its enumeration of exactly six purposes for which a user will be allowed to assert fair use rights. This constraint not only overlooks other settled categories recognized in fair use law,[220] it also cannot be squared with the text of the fair use statute, which lists illustrative but non-exclusive categories of fair use.[221] To match the experience of fair use in the offline world, the user must retain the freedom to determine not only whether, but also for what purpose, to assert a fair use right over DRM-protected content.

A rights assertion mechanism could provide users with an additional avenue to obtain access to a work, supplementing local or remote authorization mechanisms or hybrids thereof. Implementing a rights assertion capability as a supplement to a hybrid DRM mechanism of the sort championed by Professors Burk and Cohen,[222] for example, may yield a desirable combination of advantages for users while maintaining sufficient protections for copyright holders so as not to provoke their opposition.

How would such a system work in practice? First, a range of preauthorized fair uses, possibly modeled on existing safe harbors in the

218. *See supra* Part III.C.1.
219. *See infra* Parts V.C, V.D.
220. *See supra* note 214 and accompanying text.
221. *See supra* note 31 and accompanying text.
222. Burk & Cohen, *supra* note 104, at 65–70.

offline world,[223] could be encoded into the work or accompanying metadata. A user who wanted to engage in a non-preauthorized use could submit an authorization request to a remote license-issuing authority (which, for the reasons previously explored,[224] must be someone other than the copyright holder or its agent), supplying such contextual information as the system is engineered to accept. Upon approval of the user's request, the licensing authority would issue the digital keys necessary to effectuate the requested use. If, on the other hand, the licensing authority denied the request, or if the user judged the burden of applying to the license authority to be too great, the user would have still another option. The user could elect to "challenge the code"[225] and assert a right to engage in a fair use of the protected content. Faced with such an assertion of rights, a compliant player application would be required to permit the use, although it may extract a *quid pro quo* from the user in the form of contextual information for recording in an audit trail.[226]

This system would essentially allow the user to decide whether the desirability of a clear *ex ante* authorization for the intended use outweighed the burdens and privacy implications of seeking such authorization. Different users might see the issue quite differently. A textbook author might be highly motivated (or indeed, contractually bound) to secure express authorization directly from copyright holders for each piece of their content included in the textbook, rather than to simply assert fair use rights. This author might be indifferent to the

223. Although the fair use section of the Copyright Act, 17 U.S.C. § 107 (2000), includes only the four-factor "balancing test" that has been justifiably labeled impossible to automate, other copyright exceptions may be easier to encode. *See, e.g.*, 17 U.S.C. § 108 (reproduction by libraries and archives), § 110 (multiple exceptions for public performance and display of copyrighted works in various types of institutions). Other default protections may be drawn from the multipartite "Agreement on Guidelines for Classroom Copying in Not-For-Profit Educational Institutions" which appears in the legislative history of the 1976 Copyright Act as a note to § 107. The "Guidelines" carve out a series of exceptions in fairly concrete terms that may not be difficult to reduce to code, even going so far as to state precise numbers of words or exact percentages of the original source material that may be used. The "Guidelines" are intended to describe uses that are clearly fair, without purporting to cast doubt on the fairness of uses more extensive than those described — that is to say, the "Guidelines" aim to describe a floor, not a ceiling, for fair use: "The purpose of the following guidelines is to state the minimum and not the maximum standards of educational fair use under section 107 . . . . There may be instances in which copying which does not fall within the guidelines stated below may nonetheless be permitted under the criteria of fair use." H.R. REP. NO. 94-1476, at 68 (1976), *as reprinted in* 1976 U.S.C.C.A.N. 5659, 5681. An initial set of hard-coded preauthorized uses designed by analogizing to the "Guidelines," then, may be particularly appropriate for a DRM system that does not take the hard-coded defaults as exclusive, but provides other avenues to permit users to engage in further uses.

224. *See supra* notes 130–39 and accompanying text.

225. *See supra* Part IV.A.1.

226. The particular information that could be collected and the manner of its storage are issues with implications for user privacy, which will be taken up *infra* Part IV.B.2. The fact that the player program must be engineered to allow access to the content in the face of a user's assertion of fair use rights also has consequences for the design of media player hardware and software, which will be taken up *infra* Part V.C.

disclosure of identifying information that would accompany a request for such express authorization, and thus, the remote authorization mechanism might prove wholly satisfactory. Conversely, a reviewer who has been leaked a pre-release copy of a new musical album and who plans to pen an unfavorable online review, annotated with song excerpts, might be unwilling to wait for authorization and disinclined to sacrifice anonymity, perhaps for fear of jeopardizing relationships with industry sources. This user might instead bypass the authorization process in favor of simply asserting fair use rights to excerpt portions of the content. The point is simply that a DRM system engineered as described above leaves intact the user's choice whether to seek express authorization, and does so in precisely the same form that that choice takes in the offline world.

2. Identity Escrow

The proposal sketched out so far suffers from an obvious practical objection. If a user must be empowered to unilaterally assert a right to use DRM-protected content in any fashion the user wishes, and if the DRM system must be so designed as to accommodate such a request, can it still be said that the DRM mechanism *is* a DRM mechanism as that term is commonly understood? As so phrased, the question is a bit loaded; DRM mechanisms as "commonly understood" protect fair use poorly, and any effort to use DRM to legitimately limit copyright holders' exclusive rights will necessarily entail a break with past practice. Nevertheless, it is appropriate to ask how a mechanism that empowers users to do whatever they wish with content they have purchased, based solely on their own authority, differs operationally from the absence of any technological protection measure. Or, to put it slightly differently, does such a system provide to copyright owners any protection against widespread infringement by users determined to infringe?

The answer is yes, up to a point. That point is actually fairly solicitous of copyright holder interests — far more so, indeed, than exists as a practical matter in the offline world. It is, however, a less extensive protection than the effective lockdown that current DRM implementations promise (even if they ultimately fail to deliver) to copyright holders.

What differentiates a DRM system designed to protect fair use on the one hand from the absence of DRM on the other is the potential existence of a permanent record of user rights assertions. LicenseScript's authors refer to this record as the "audit trail," whose very name suggests policing users to ensure that their zeal to use copyrighted works does not devolve into unchecked infringement. This terminology seems tolerably apt, and I will continue to use it,

although as the ensuing discussion will reflect, my conception of the audit trail departs from LicenseScript's in some respects.

Many observers have expressed concern about the capabilities of contemporary DRM systems to erode user privacy.[227] Professor Cohen has suggested that DRM infrastructure be designed to minimize the collection of user-identifying information.[228] To avoid the risk that disclosure of a user's personal information will intrude upon the legitimate sphere of privacy that ordinarily surrounds personal uses of copyrighted works, DRM systems should not even collect such information except where indispensable to some instrumental function:

> Value-sensitive design for DRM also would investigate methods of building in limits on monitoring and profiling of individual users. Because most businesses need to collect and retain some information about their customers to manage orders, payments, and deliveries, technological limits on data collection and use cannot fully substitute for other, human-implemented safeguards. Nonetheless, DRM systems may be designed either to minimize or to maximize data collection, retention, extraction and use. To preserve the intellectual privacy of information users, DRM design should incorporate minimization principles.[229]

Professor Cohen's basic point is that merely because detailed user information can be collected by a DRM system, it does not follow that it should be. Instead, it is pertinent to ask at each stage of the process whether the collection of user data is justified in light of some instrumental aim. Collection and retention of more information than is necessary heightens the risk to user privacy, and should be avoided for that reason alone.[230]

Assuming that some information must be collected in order for the DRM system to function, can sufficient protections be implemented to prevent information collection from impairing user privacy? A recent article, provocatively titled *Privacy-Preserving Digital Rights Management*, aims to answer that question in the affirma-

---

227. *See, e.g.*, Jonathan Zittrain, *What the Publisher Can Teach the Patient: Intellectual Property and Privacy in an Era of Trusted Privication*, 52 STAN. L. REV. 1201, 1243–45 (2000).

228. Julie E. Cohen, *DRM and Privacy*, 18 BERKELEY TECH. L.J. 575, 612 (2003).

229. *Id.* at 611–12 (footnote omitted).

230. *See supra* notes 189–91 and accompanying text.

tive.[231] The technical details of the proposal are beyond the scope of this essay, but its essential thrust may be grasped readily enough. At each stage of the interaction between a user and a license-issuing authority in a DRM system, the parties interact not directly, but through pseudonymous intermediaries — essentially, digital certificates that are issued to facilitate a given interaction, but from which the user's identity cannot be deduced:

> In the basic privacy-preserving DRM ["P2DRM"] system, the real identity of the user is decoupled from identifiers which the user possesses in the system. These identifiers, i.e. user pseudonyms . . . are used to link a user . . . to content, thus allowing a user to access the content for which he bought the rights . . . .
>
> . . . .
>
> The basic privacy threat that P2DRM circumvents is the association of a user's real identity and content that the user owns, association which may happen with the use of personal licenses for content access. This also prevents that users are tracked while accessing the content.[232]

The authors' description of how a user would interact with a license-issuing authority in this fashion is generic enough to be applied to any of the interactions that would be necessary to implement the various DRM mechanisms discussed above. The basic structure would resemble the following:

> 1. A user purchases some type of identification device (perhaps a "smart card") from a retailer. Embedded in this device is an encryption key pair consisting of a public key and a secret key.[233]
>
> 2. User inquiries concerning the availability of various content (or licenses in a DRM system of the type I have been describing) are conducted via an anonymous channel through which the parties can negoti-

231. Claudine Conrado et al., *Privacy-Preserving Digital Rights Management*, *in* SECURE DATA MANAGEMENT: VLDB 2004 WORKSHOP, SDM 2004, LNCS 3178, at 83 (Willem Jonker & Milan Petković eds., 2004).

232. *Id.* at 85.

233. *See generally* Wikipedia, *Public-key Cryptography*, http://en.wikipedia.org/wiki/Public-key_cryptography (as of Nov. 17, 2006, 00:49 GMT).

> ate terms without the content provider learning the user's identity.
>
> 3. If the parties agree to the terms of an exchange, the anonymous intermediary completes any required payment, and then supplies the content provider with the user's public key, which the content provider uses to encrypt the content (or license). The content provider then returns the encoded content to the anonymous intermediary, which in turn forwards it to the user.
>
> 4. The user decodes and uses the supplied content with the secret key from the user's identification device.[234]

This approach is not perfectly secure. The content provider does, as a result of the transaction, learn which public key is associated with a given request for the particular content. Because the public key was supplied to the content provider through the anonymous channel, however, the content provider does not learn the user's identity.[235] Another possibility, not discussed in the article, is that a particular request, even though conducted through an anonymous channel, will supply information sufficient to allow the content owner to deduce the requester's identity. Preventing a clever licensor from piecing together what is known of a given user request (perhaps concerning some specialized or idiosyncratic work that is of interest to a finite and known pool of potential users) and deducing the identity of the user behind the request is probably impossible, and the risk exists even under the authors' "privacy-preserving DRM" proposal.

The authors go on to expand their proposal to address other scenarios, such as an anonymous transfer of a license from one user to another, and revocation of a license grant in which the licensor does not know the licensee's identity.[236] Nevertheless, the basic point for

---

234. *See* Conrado et al., *supra* note 231, at 86–90. Certain steps from the authors' description of their process have been omitted in the interest of brevity, although at the possible risk of introducing ambiguity that is not present in the original.

Another proposal that follows the same general format is available in Seki & Kameyama, *supra* note 20, at 4113–14. This proposal adds complexity to the design by encrypting each exchange of keys and content with one-time session keys that expire upon use. This is offered as a way of reducing the risk that an eavesdropper situated in the network between the sender and the recipient could monitor the parties' encrypted communications and deduce the encryption scheme they are employing (the so-called "man in the middle attack"). The underlying structure of the proposal, however (transmittal of an anonymous public key that is then used to encrypt either the content or a separate key necessary for playback) is essentially the same as in the Conrado et al. article.

235. Conrado et al., *supra* note 231, at 87.

236. *Id.* at 90–93.

present purposes remains unchanged. User privacy is preserved at each stage of the process by barring disclosure of enough information to allow any participant to deduce which individual user is associated with a given public key. Indeed, the authors point out, deducing the user's identity from the public key ought to remain impossible even if all other participants in the system collude and share what information they possess about the portions of each transaction in which the user has engaged.[237]

What lessons can be drawn from this model for the creation of a DRM system that is protective of both fair use and user privacy? Accepting for present purposes the need for an audit trail to discourage users from infringing copyrights, the foregoing examples nevertheless suggest ample room for improvement over the privacy-defeating design of LicenseScript. The basic design problem is an issue of conflicting imperatives: requiring some record of assertions of fair use rights so that users do not believe they are completely unsupervised, while minimizing the disclosure of user-identifying information to copyright holders.

One approach would be to record in the audit trail various contextual information about an asserted fair use *except* for the user's identity. The user's identity could instead be represented by the user's public key, as the public key substitutes for the user's identity for most interactions in the "privacy-preserving DRM" system. As Conrado et al. suggest, it should remain impracticable to deduce the user's identity from the public key (or, to be more precise, from the combination of the public key and the transactional information held by the other participants in the system).[238]

A user who was perfectly confident that the content provider could never discover her identity would lack any obvious incentive to refrain from using the DRM system's rights assertion tools to infringe copyright. Accordingly, rather than being designed not to collect user identification information, a DRM system engineered for fair use could collect such information, but hold it in escrow, entirely separate from the audit trail. To the copyright holder's eyes, only a stream of digits (that is, the public key) would identify a party who had asserted fair use rights in DRM-protected digital content. If its review of the

---

237. *Id.* at 97–99. The authors note that the distribution of information about the user and the transactions in which she engages should suffice to prevent discovery of the user's actual identity even if all the parties other than the user collude. The smart card issuer at Step 1 of the process outlined in the text, for example, does not know what key has been encoded on the card purchased by any user. The content provider at Step 2 of the process learns the connection between the user's public key number and the content the user has accessed (or the rights the user has acquired), but no other information. The intermediary knows the user's public key and which information or rights the user has accessed. But in theory, the critical connection — between the user's public key and the user's own identity — remains unknown to all parties except the user herself.

238. *Id.* at 87.

audit trail gave reason to believe that substantial infringement was occurring, a copyright holder could secure the release of the user's actual identity from escrow, much as a copyright holder can now compel internet service providers to divulge the identities of users who are believed to be committing copyright infringement.[239] The particulars of the identity release procedure need not be fully developed here; the point for present purposes is simply that an identity-escrow scheme could satisfy copyright holders' needs to police abuses of the rights assertion framework that are detected within the audit trail while simultaneously guaranteeing user privacy in the ordinary operation of the system.

3. Summary

The combination of a robust rights assertion framework with the privacy-preserving characteristics of identity escrow could go a long way towards addressing the lingering concerns by effectively protecting fair use in DRM. Unlike local authorization, remote authorization, and hybrid DRM mechanisms, a DRM system that empowers users to assert fair use rights to access protected content would prevent fair use from collapsing into *authorized* use, thereby preserving the viability of fair uses to which the copyright owner objects, just as in the offline world. Empowering rights assertion by users may also restore spontaneous fair uses. By withholding personally identifying information in ordinary operation, moreover, such a system would minimize the chilling effects that inevitably result when one is certain that one's identity and one's fair use will become known.

The system also protects the needs of copyright holders through the mechanism of the audit trail — a form of protection that copyright holders do not enjoy in the offline world. The identity escrow provision protects copyright holders' interests in squelching abuses of the rights assertion system. Following a sufficient showing of possible infringement (based on the audit trail), the copyright holder would become entitled to pierce the veil of public-key pseudonymity and learn the user's identity.

Earlier in this Article, I chose user experiences with fair use in the offline world as the benchmark against which to evaluate protections for fair use in DRM systems.[240] My proposal improves upon the competing proposals I have previously discussed, but it is not without flaws. The weakest point is the audit trail logging of information concerning fair use rights assertions. Even if one accepts the necessity of that logging mechanism as a deterrent to abuses of the rights-assertion process, the audit trail nevertheless has no parallel in the offline

239. *See* 17 U.S.C. § 512(h) (2000).
240. *See supra* Part II.A.

world.[241] Users particularly sensitive to the risk of disclosure of identifying information might find the identity escrow system an insufficient layer of protection, and thus not engage in precisely the types of uses the system is meant to foster. These are substantial concerns, and I do not mean to minimize them by noting that they are present in at least the same degree (and often, to a far greater degree) in the various predecessor proposals to which my alternative responds. Whether perfection as I have defined it is ultimately attainable or not, it is certainly possible to move closer to it than existing DRM systems have.

To be sure, a system of the type outlined in this section promises a number of improvements over the status quo. But is it achievable? The answer to that question will require consideration of possible reforms in areas as varied as law and software design, and it is to that final topic that I now turn.

V. CHALLENGES FOR IMPLEMENTATION: HARNESSING THE MODALITIES OF REGULATORY CHANGE[242]

Part IV.B sketched out a proposal that would increase protections for fair use rights in DRM technologies by empowering users to assert fair use rights over purchased content irrespective of the wishes of the copyright holder. To deter abuse, the system would preserve a record of the asserted fair uses in the form of an audit trail. The audit trail would record what uses had been made of the protected content and the user's stated grounds for claiming fair use protections, but would not record any information identifying those users who had asserted fair use rights. Any user-identifying information would be escrowed with a third party and revealed to the copyright holder only upon a showing of cause. We might label such a DRM mechanism "fair use-friendly."[243]

Implementing such a proposal may substantially improve the ability to exercise fair use rights, which is a desirable outcome from a policy standpoint. Granting users the technological capability to engage in fair uses of DRM-protected works would bring practical reality back in line both with the existing law and with settled user expectations derived from long experience with fair uses of offline works. Improving protections for fair use in DRM would also eliminate one of the strongest criticisms of the DMCA and re-ground that legislation in its original purpose of deterring copyright infringement.

---

241. *Cf. supra* notes 189–91 and accompanying text.

242. *See* LAWRENCE LESSIG, CODE AND OTHER LAWS OF CYBERSPACE 87–89 (1999) (discussing behavior-constraining force exerted by law, norms, markets, and architecture as distinct modalities of regulation).

243. *See* Barbara Fox, Fair Use Friendly DRM? (2002), http://www.cfp2002.org/fairuse/fox.pdf.

Empowering users to exercise their fair use rights without violating the DMCA might, in turn, increase law-abiding behavior[244] and temper the critical evaluation of the DMCA as a one-sided giveaway to powerful producer cartels.[245] It would eliminate the anomalous situation in which private entities are effectively empowered to rescind a legislative grant of rights to the public at large. Finally, re-empowering users to engage in fair uses of digital media could spark a storm of new creative output — valuable both for its own sake and for the new market opportunities it could yield — as transformative uses of content previously forbidden by technology would again become possible.[246]

This would be a very different world from the one we presently inhabit — sufficiently different to raise nontrivial doubts whether it could feasibly come to exist. Because of the benefits that would be available to users of digital media if DRM technologies incorporated stronger provisions for fair use rights, it is worth exploring, at least tentatively, what would be required to effect such change.

A. Social Norms

Perhaps the single most important precondition for the adoption of fair use-friendly DRM is neither legal nor technological, but cultural. The emergence of a public consensus that DRM should protect fair use, and that a technological lockdown of creative works is no longer acceptable, will do much to spur reform.

Efforts to increase public awareness of the social costs imposed by the current legal and technological regime are already underway. Professor Lawrence Lessig's recent books *Free Culture*[247] and *The Future of Ideas*,[248] for example, are accessible efforts to demonstrate to nonspecialist audiences the shortcomings of the current system. Indeed, a growing body of critical literature has begun to emerge in recent years highlighting the harm to the public welfare caused by an intellectual property regime that cedes to copyright holders too much control over how their works are used.[249] This literature, in turn, is

---

244. *See* Dhamija & Wallenberg, *supra* note 73, at 17 ("DRM extension proposals . . . may increase user compliance, because users are now able to engage in fair use without circumvention.").

245. *See, e.g.*, Richard M. Stallman, *Misinterpreting Copyright —A Series of Errors*, *in* FREE SOFTWARE, FREE SOCIETY: SELECTED ESSAYS OF RICHARD M. STALLMAN 77, 82–83 (Joshua Gay ed., 2002), *available at* http://www.gnu.org/philosophy/fsfs/rms-essays.pdf.

246. *See* LAWRENCE LESSIG, FREE CULTURE: THE NATURE AND FUTURE OF CREATIVITY (2004).

247. *Id.*

248. LAWRENCE LESSIG, THE FUTURE OF IDEAS: THE FATE OF THE COMMONS IN A CONNECTED WORLD (2001).

249. *See, e.g.*, FISHER, *supra* note 4; RICHARD M. STALLMAN, FREE SOFTWARE, FREE SOCIETY: SELECTED ESSAYS OF RICHARD M. STALLMAN (Joshua Gay ed., 2002); LITMAN,

itself a current in a broader stream of scholarship that has begun to question (or, in some instances, to renew old questions about) the state of intellectual property law more generally.[250] This is a time of growing academic interest in the linkages between copyright law and policy on the one hand, and individual creative liberty on the other.

Outside the academic community, citizen groups have arisen to advocate copyright reform and foster greater awareness of intellectual property issues.[251] These groups broaden the debate beyond college campuses, bringing new voices into the mix. In time, they may shift public attitudes and inspire calls for reform, including stronger protections for fair use. While these groups are now fringe players, far removed from political and economic power and lacking day-to-day influence over policy, increases in protections for user rights will likely begin with them.

The Creative Commons project offers a number of different licenses — essentially, contractual alternatives to copyright — that creative artists may adopt when issuing their content.[252] Some of these licenses expressly permit users to engage in activities that would otherwise constitute copyright infringement. Indeed, the avowed goal of the project is to enlarge the scope of the commons, the shared pool of cultural antecedents upon which future creators may draw for their own work. In some respects, the project is expressly about influencing the role that cultural norms play in shaping users' everyday interactions with creative content,[253] allowing users to become active participants in the back-and-forth of creative dialogue, rather than passive consumers of content owned by corporate media conglomerates and locked up with DRM. Creative Commons is an experiment and a work in progress. If it bears fruit, it may demonstrate that a vibrant process of creative production is sustainable even when the ordinary controls of copyright law are relaxed.

It is not difficult to envision ways in which projects like Creative Commons could influence cultural norms concerning legal and technological protections for copyrighted works. If users of Creative

---

supra note 4, chs. 10–13; SIVA VAIDHYANATHAN, COPYRIGHTS AND COPYWRONGS: THE RISE OF INTELLECTUAL PROPERTY AND HOW IT THREATENS CREATIVITY ch. 5 (2001).

250. *See, e.g.*, ADAM B. JAFFE & JOSH LERNER, INNOVATION AND ITS DISCONTENTS: HOW OUR BROKEN PATENT SYSTEM IS ENDANGERING INNOVATION AND PROGRESS, AND WHAT TO DO ABOUT IT (2004); JAMES BOYLE, SHAMANS, SOFTWARE, AND SPLEENS: LAW AND THE CONSTRUCTION OF THE INFORMATION SOCIETY chs. 4–6, 13 (1996).

251. *See, e.g.*, Public Knowledge, http://www.publicknowledge.org (last visited Nov. 16, 2006); Downhill Battle, http://www.downhillbattle.org (last visited Nov. 16, 2006). For international counterparts to these groups, see, for example, Consumers Digital Rights Campaign, http://www.consumersdigitalrights.org/cms/index_en.php (last visited Nov. 16, 2006) and Online Rights Canada, http://www.onlinerights.ca (last visited Nov. 16, 2006).

252. Creative Commons Licenses, http://creativecommons.org/about/licenses/meet-the-licenses (last visited Nov. 16, 2006).

253. *See* Christopher M. Kelty, *Punt to Culture*, 77 ANTHROPOLOGICAL Q. 547, 553–54 (2004).

Commons-licensed media become accustomed to being able to engage in transformative uses of content they have purchased, for example, they may become less tolerant of a legal and technological regime that denies them comparable fair use rights in traditional DRM-protected digital media. In other words, the success of projects like Creative Commons could fuel consumer demand for a relaxation of DRM restrictions. In the face of such demand, strengthening accommodations for fair use in DRM would be an achievable goal that content providers could adopt.

For consumers and citizens to demand greater protections for fair use, they must develop a sense of how they are harmed by the comparative absence of such protections under the current regime. While the intellectual and organizational foundations for such a shift in public attitudes are being laid, it is too soon to know whether those foundations ultimately can support enduring pro-user social norms and revitalize the scope of fair use protections. Nevertheless, the work now underway is certain to be an indispensable part of any such evolution.

B. Markets

The paucity of market-centric approaches for protecting end user rights in DRM is puzzling. To be sure, there have been proposals that aim to incorporate market mechanisms to solve digital copyright problems in innovative ways, such as the proposal to give content owners a positive stake in the spread of peer-to-peer technology by compensating them for each transfer of one of their works on such services.[254] Absent, however, has been any suggestion that a business model could be devised that increases a copyright holder's rewards in proportion to the technological protections it provides for fair use of its works.

It is not intuitively clear why this should be so. The success of Apple Computer's comparatively permissive iTunes Store,[255] for example, suggests that consumers will reward sellers who use less restrictive technologies to protect the content they sell. Offering robust provisions for fair use, instead of the weak ones now widely available,

---

254. *See, e.g.*, Jürgen Nützel & Rüdiger Grimm, *Potato System and Signed Media Format — An Alternative Approach to Online Music Business*, *in* PROCEEDINGS OF THE 3RD INTERNATIONAL CONF. ON WEB DELIVERING OF MUSIC 23 (2003), http://www.4friendsonly.org/papers/Nuetzel_Potato_Webdelmusic03.pdf. *See generally* Digital Media Project, Berkman Center for Internet & Society, Content and Control: Assessing the Impact of Policy Choices on Potential Online Business Models in the Music and Film Industries (2005), http://cyber.law.harvard.edu/media/files/content_control.pdf (analyzing how four different business models could be applied to digital media).

255. *See supra* note 61–64 and accompanying text.

would provide an exceptional way for a seller of digital content to distinguish itself from its competitors and build market share.

The problem, however, may lie not with the technology developer or reseller, but with the copyright holder upstream. The recorded entertainment industries are characterized by oligopolistic interdependency. Moreover, copyright holders generally hold no great enthusiasm for fair use. Suppliers of recorded entertainment in particular have been dragged forcibly onto the Internet, loudly protesting and litigating at each step of the way to preserve old revenue streams and business models.[256] As between a system offering strong DRM with minimal protections for fair use, and a DRM system that protects fair use but which may be abused by users to infringe copyright, experience suggests that the content industries would favor the former. A technology reseller that offered a fair use-friendly DRM system might very well attract customers. But it would have little content to offer them.

At present, market mechanisms may provide little incentive for copyright holders to embrace DRM technologies engineered for fair use. Whether novel business approaches can be developed to encourage them to do so, just as authors have begun to propose approaches for reconciling the content industries with peer-to-peer distribution, remains outside the scope of this Article, but suggests a potentially fruitful avenue for further legal, economic, and technological research.

C. Code

Adopting a DRM system engineered for fair use will have important ramifications for design of the hardware and software that provide user access to DRM-protected digital media. These ramifications, in turn, are likely to provoke the strongest political objections to fair use-friendly DRM. In my opinion, these objections are indistinguishable as a practical matter from objections to fair use *per se*, so I will not treat them separately in this section. The possible benefit of a public dialogue on fair use more generally, however, will be considered in the next section when addressing possible legislative initiatives.[257]

The most substantial and visible technological changes will involve implementing a user rights assertion mechanism in code. From the user's view, the defining characteristic of a DRM system engineered for fair use is the increased range of possible uses that are implemented in its controlling hardware and software. For the reasons explored previously, a DRM system may be said to protect fair use

256. *See* FISHER, *supra* note 4, ch. 3.
257. *See infra* Part V.D.

precisely to the extent that its programming allows it to recognize and act upon a user's unilateral assertion of rights.

The primary consequence of this design decision is that the media player component in a fair use-friendly DRM system must, at some point, be able to accommodate any request a user makes — even uses that are determined *ex post* to be illegal. Because the fair use doctrine sometimes permits duplication of an entire work, for example, the DRM mechanism must be technically capable of duplicating the entire work in response to a user's assertion of fair use rights. Similarly, it must be capable of extracting arbitrary subparts of the whole at the user's request. It need not offer these capabilities by default, but once the user has asserted the fair use right, the DRM system must comply.

One alternative would be to embed the technological capability of unrestricted playback and duplication in every media player, and unlock that functionality with respect to a particular item of media upon the user's assertion of fair use rights. This design would satisfy the requirements of fair use-friendly DRM, but would obviously be more susceptible to circumvention: sufficiently proficient users could tweak the code to make unrestricted playback the default. Content suppliers might be forgiven for viewing such a design as, at best, suboptimal.

Erickson and Mulligan suggest an alternative.[258] Software players might be designed modularly, with capabilities that could be extended in response to a user's assertion of fair use rights. In their terms, upon a user's assertion of fair use rights, a compliant player might be designed to "deliver to individuals technical capabilities not previously installed" in the player mechanism.[259]

There is an (admittedly inexact) analogy to just this sort of modularity in the design of existing media players. A wide variety of data compression schemes exist for the encoding of both audio and video content.[260] It is common for personal computer media player programs, upon encountering an audio or video file that has been encoded with an unfamiliar compression scheme, to download from the Internet whatever additional software is necessary to process the user's request. The player program, in other words, extends its own capabilities to accommodate a user's request to play back encoded content.

A modular player mechanism might be developed in similar fashion to support fair use rights in DRM. Although a player application might be designed *ab initio* (as most commercial programs currently are) to limit user interactions with DRM-protected content to a range

---

258. Erickson & Mulligan, *supra* note 102, at 995.

259. *Id.*

260. *See* Wikipedia, *List of Codecs*, http://en.wikipedia.org/wiki/List_of_codecs (as of Nov. 17, 2006, 01:17 GMT).

of preauthorized permissible uses, the player could be engineered to recognize a user's assertion of additional fair use rights, and to respond accordingly by extending its own capabilities, at least temporarily. The player could be designed to self-install whatever additional functionality is needed to comply with the user's assertion of rights.

The foregoing example is only one possibility, hypothesized by a nonspecialist, of how a mandate to strengthen protections for fair use in DRM technology might alter the design of computer software. I do not intend to suggest that the specific design described above should be mandated by law because legislative or regulatory "technology forcing" threatens perverse and unintended consequences. If the goal of improving protections for fair use in DRM were mandated, however, an extensible media player tool might be one of the technologies that could evolve to fill the need. The next subsection investigates how legal tools might be employed to press for such an improvement in fair use protections for digital media.

D. Law

Reinterpreting the DMCA. I previously noted that the tension between the fair use doctrine and the reality of technological restrictions on user rights flowed partly from restrictive judicial interpretations of the DMCA. Those interpretations, in my view, are not commanded by the statutory text and appear inconsistent with the stated legislative purpose behind the DMCA.[261] The Supreme Court has never approved these prior judicial constructions of the statute, and the majority of the circuit courts have never opined on the DMCA. Therefore it is possible that conditions more favorable to the protection of fair use in DRM could come about through future judicial interpretations of the DMCA more accommodating of fair use rights.

This prospect is not merely academic. Although early judicial interpretations of the DMCA tended to take a restrictive view of users' rights in general and fair use in particular,[262] more recent decisions have recognized a more expansive sphere of user rights to circumvent DRM mechanisms in some circumstances.[263]

In *Chamberlain Group, Inc. v. Skylink Technologies, Inc.*, a manufacturer of electronic remote-control garage door openers al-

261. *See supra* Part II.B.3.

262. *See, e.g.,* Universal City Studios, Inc. v. Reimerdes, 111 F. Supp. 2d 294, 321–24 (S.D.N.Y. 2000), *aff'd sub nom.* Universal City Studios, Inc. v. Corley, 273 F.3d 429 (2d Cir. 2001); RealNetworks, Inc. v. Streambox, Inc., No. 2:99CV02070, 2000 WL 127311, at *8 (W.D. Wash. Jan. 18, 2000).

263. *See, e.g.,* Lexmark Int'l, Inc. v. Static Control Components, Inc., 387 F.3d 522, 531–32, 546–49 (6th Cir. 2004) (holding that DMCA did not empower manufacturer of laser printers to inhibit competition in the aftermarket for refilled toner cartridges by embedding an electronic "authorization mechanism" in its printers that was "circumvented" by makers of refilled toner cartridges).

leged that a competitor had "circumvented" its proprietary code sequence to create a "universal" transmitter that worked with many other manufacturers' garage door mechanisms.[264] The court rejected the allegation that, in so doing, the competitor had violated the DMCA.[265] The *Chamberlain* court cautioned against interpreting the DMCA "to restrict consumers' rights" by "allow[ing] any manufacturer . . . to add a single copyrighted sentence or software fragment to its product, [and] wrap the copyrighted material in a trivial 'encryption' scheme" that users would then be barred from circumventing.[266] And in a passage that could presage much more lenient judicial constructions of the DMCA in the future if carried to its logical conclusion, the *Chamberlain* court did what other courts had expressly refused to do: it measured the reach of the DMCA's anti-circumvention bar based in part on its effect on other rights granted to users under the copyright laws:

> The DMCA . . . *defines* circumvention as an activity undertaken "without the authority of the copyright owner." The plain language of the statute therefore requires a plaintiff alleging circumvention (or trafficking) to prove that the defendant's access was unauthorized — a significant burden where, as here, the copyright laws authorize consumers to use the copy of Chamberlain's software embedded in the [garage door openers] that they purchased.[267]

Read literally, *Chamberlain* seems to suggest that circumvention of a DRM mechanism does not violate the DMCA where "the copyright laws authorize consumers to use the [content] that they purchased" in the desired fashion.[268] It would be a small step indeed to conclude that circumventing DRM is not punishable when it enables fair use of the underlying content, and in time, evolving judicial attitudes may lead courts to such a conclusion.[269]

---

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

265. *Id.* at 1202–03.

266. *Id.* at 1201.

267. *Id.* at 1193 (citation omitted).

268. *Id.*

269. The facts of *Chamberlain* suggest one potentially crucial distinction. *Chamberlain* arose in the context of a dispute between a producer of durable goods and its economic competitor. *See id.* at 1183. Where the DMCA is invoked as a tool to squelch economic competition, courts have not generally seen fit to intervene. *See, e.g.*, Monotype Imaging, Inc. v. Bitstream, Inc., 376 F. Supp. 2d 877 (N.D. Ill. 2005); Agfa Monotype Corp. v. Adobe Sys., Inc., 404 F. Supp. 2d 1030 (N.D. Ill. 2005). On the other hand, in cases closer to copyright's heartland, courts might well give the DMCA a broader reading in the interest of protecting creative media works such as music, films, or software. *See, e.g.*, Davidson & Assocs. v. Jung, 422 F.3d 630, 640–42 (8th Cir. 2005).

Such an evolution is on display in *Storage Technology Corp. v. Custom Hardware Engineering & Consulting, Inc.*, in which the same court, drawing upon *Chamberlain*, again rejected a DMCA claim in the durable goods context.[270] There, an outside service and repair firm performed maintenance work on a tape data storage library manufactured by plaintiff Storage Technology Corporation ("StorageTek"). As part of its maintenance work, defendant Custom Hardware Engineering ("CHE") employed two devices to intercept copyrighted maintenance and diagnostic codes built into StorageTek's products. The court first rejected StorageTek's argument that CHE infringed its copyrights in the code, reasoning that CHE inherited the statutory authority of StorageTek's customers to copy the code for purposes of maintenance and repair.[271] Then, in a passage with potentially far-reaching implications, the court reasoned that the failure of StorageTek's copyright claim *ipso facto* doomed any claim under the DMCA:

> To the extent that CHE's activities do not constitute copyright infringement or facilitate copyright infringement, StorageTek is foreclosed from maintaining an action under the DMCA. That result follows because the DMCA must be read in the context of the Copyright Act, which balances the rights of the copyright owner against the public's interest in having appropriate access to the work. Therefore, courts generally have found a violation of the DMCA only when the alleged access was intertwined with a right protected by the Copyright Act. To the extent that StorageTek's rights under copyright law are not at risk, the DMCA does not create a new source of liability.[272]

Continued evolution in the same direction may, in time, lead courts to a position that is more hospitable to fair use. Were courts to hold that users may circumvent DRM mechanisms for the purpose of making fair use of a protected work without incurring liability under the DMCA, it would, as a practical matter, enlarge the sphere of possible fair uses that could occur without the danger of such liability.

Nevertheless, it probably is not sufficient to rely on changing judicial attitudes to redress the imbalance that presently exists between the extent of fair use permitted by law and the extent that DRM tech-

---

270. Storage Tech. Corp. v. Custom Hardware Eng'g & Consulting, Inc., 421 F.3d 1307 (Fed. Cir. 2005).

271. *Id.* at 1311–15 (citing 17 U.S.C. § 117(c) (2000)).

272. *Id.* at 1318 (citations omitted).

nology makes practicable. Easing the threat of DMCA liability benefits that subset of users who possess the technological proficiency necessary to circumvent DRM mechanisms. Other users, however, must content themselves with the limitations of the DRM or else seek out devices to assist in circumvention — a burden that some users will no doubt conclude is not worth the trouble even if circumvention would be lawful in that instance.[273]

Regulatory Responses. I raise this possibility principally to draw attention to its conspicuous absence from the terms of the debate. Thus far, Congress has declined to grant any regulatory agency the authority to define fair uses of copyrighted works or to regulate the technologies of access control.[274] One can envision regulatory structures that would promote broader protections than presently exist for fair use in DRM, but the practical foundations for such structures do not yet exist.

Legislative Responses. Legislation is presently the most promising avenue toward strengthening protections for fair use of DRM-protected content. To date, Congress has taken little notice of the effects of emerging DRM technologies on fair use. Although Congress disclaimed any intent to circumscribe the fair use doctrine when it enacted anti-circumvention protections for DRM technologies,[275] it has so far acquiesced in judicial interpretations of the DMCA that effectively constrain fair use.

What actions might Congress take to improve the protection for fair uses of DRM-protected digital works? One possibility would be to mandate or prohibit the use of specific types of DRM technologies by fiat, although I have previously suggested that this may be an unat-

---

273. Even this latter possibility, of course, presupposes the availability of circumvention devices, a prospect that may be far from assured given the risk that developers of such devices may be held secondarily liable if their device is ultimately used, or publicly claimed to be potentially useful, to infringe copyrights. *See* Metro-Goldwyn-Mayer Studios Inc. v. Grokster, Ltd., 545 U.S. 913 (2005). The risk that a device developer may be held secondarily liable for its users' infringing acts is no doubt a disincentive to the creation of circumvention devices. *Cf.* Fox & LaMacchia, *supra* note 95, at 63.

274. The closest that Congress appears to have come is a provision in the DMCA that authorizes the Librarian of Congress, in consultation with the Register of Copyrights, to promulgate exceptions to the broad statutory ban on circumventing technological protection measures. 17 U.S.C. § 1201(a)(1)(C)–(D) (2000). The Library's use of this authority to date, however, has been cautious — indeed, some would say, overcautious — and has not placed the Library of Congress at the heart of digital media regulation in the same way that other federal agencies dominate the creation and enforcement of substantive law within their various domains. For an argument that the Library's statutory powers have thus far been ineffective to protect fair use against encroachment from the DMCA's anti-circumvention provisions, see Woodrow Neil Hartzog, *Falling on Deaf Ears: Is the "Fail-Safe" Triennial Exemption Provision in the Digital Millennium Copyright Act Effective in Protecting Fair Use?*, 12 J. INTELL. PROP. L. 309, 314 (2005). Absent a clearer delegation from Congress, it is unclear whether any agency presently enjoys regulatory jurisdiction over digital media and related technologies. *See, e.g.*, *supra* note 66.

275. *See* 17 U.S.C. § 1201(c)(1) (2000).

tractive option. Amending the DMCA to permit DRM circumvention for the purpose of making noninfringing uses of the underlying content is another possibility,[276] although from the perspective of the would-be fair user, this alternative probably includes insufficient *ex ante* assurance of nonliability.[277] More durable change, however, might be achieved by establishing goals or objectives that would induce, rather than command, the adoption of particular technologies protective of fair use. Currently, copyright holders probably have few incentives to include protections for fair use in DRM technologies; however, legislative action could supply adequate incentives to encourage the inclusion of such protections.

Congress has many tools available to induce the development of DRM technologies protective of fair use. For example, it could condition some of the rights and privileges available to copyright holders on their deployment of adequate tools for the protection of fair use. The Berne Convention would presumably prohibit Congress from conditioning copyrightability on the presence of adequate fair use protections in any DRM system deployed to protect the work,[278] but the enforceability of a copyright on a DRM-protected digital work in United States courts could be made contingent upon the presence of adequate protections for fair use in the DRM mechanism.[279] Congress also could condition enforceability of the DMCA's anti-circumvention provision on the presence of adequate technological protections for fair use in any DRM mechanism that controls access to the underlying copyrighted work.[280]

Congress might also look to the European Union Copyright Directive ("EUCD") as a source of analogous authority for strengthening protections for fair use. Article 6(4) of the EUCD imposes a duty on copyright holders not to make noninfringing access to their works impossible:

---

276. Such a proposed amendment is currently before the House Subcommittee on Commerce, Trade and Consumer Protection. *See* H.R. 1201, 109th Cong. § 5(b)(1) (2005). This is also the approach taken in the most recent Canadian proposal on the enactment of statutory protections for DRM technologies. *See* Department of Canadian Heritage, Copyright Policy Branch, Government Statement on Proposals for Copyright Reform — Frequently Asked Questions (July 5, 2005), http://pch.gc.ca/progs/ac-ca/progs/pda-cpb/reform/faq_e.cfm ("[T]he circumvention of a [technological measure] applied to copyrighted material will only be illegal if it is carried out with the objective of infringing copyright.")

277. *Cf.* LESSIG, *supra* note 246, at 187–88 (arguing that overly protective copyright rules, which are removed from the original conceptions of copyright, stifle creative expression).

278. Berne Convention for the Protection of Literary and Artistic Works, Sept. 9, 1886, 25 U.S.T. 1341, 828 U.N.T.S. 221 (in original form), 1161 L.N.T.S. 3 (as revised 1971 and 1979). Article 5(2) of the Berne Convention provides, in relevant part, that "[t]he enjoyment and exercise of [a copyright holder's exclusive] rights shall not be subject to any formality."

279. *See* Burk & Cohen, *supra* note 104, at 65. The authors' proposal analogizes from the present requirement of United States law that requires registration of a copyrighted work as a precondition to bringing suit for infringement. *See* 17 U.S.C. § 411(a) (2000).

280. Burk & Cohen, *supra* note 104, at 66.

> [I]n the absence of voluntary measures taken by rights holders, including agreements between rightholders and other parties concerned, Member States shall take appropriate measures to ensure that rightholders make available to the beneficiary of [a copyright] exception or limitation . . . the means of benefiting from that exception or limitation, to the extent necessary to benefit from that exception or limitations and where the beneficiary has legal access to the protected work . . . concerned.[281]

This provision, if read literally, comes close to enacting what Professor Lessig labels "copy-*duty*," the flip side of copyright — "the duty of owners of protected property to make that property accessible."[282] This is a novel approach to reconciling the historical rights of users to engage in fair uses of copyrighted works with the increased powers of technological control DRM makes available to copyright holders. As one commentator observed, the EUCD "is certainly the first time in European copyright law that authors have been asked to facilitate the exercise of exceptions to their own rights."[283]

There may, however, be less here than meets the eye. The EUCD's stated preference for voluntary action (including agreements) may leave copyright holders with room essentially to contract around the protections the Directive is meant to supply, subject to whatever further constraints individual EU member nations may mandate. The Directive provides little guidance to individual EU nations on the particular steps they might take if rightholders are not believed to be providing adequate protections, or indeed on how to ascertain whether such protections are adequate or not.[284] Furthermore, Article 6(4) of the EUCD does not insist that *every* copyright exception remain technologically available, but only a subset consisting of seven particular exceptions that are cross-referenced in the Directive. The exceptions that must remain available to users of DRM-protected works include some that would be recognized as similar to fair use under American law, such as the exception in Article 5(3)(a) of the EUCD for uses "for teaching or scientific research."[285] But others that American law would also consider to involve fair use, such as news reporting or par-

---

281. Council Directive 2001/29/EC, art. 6(4), 2001 O.J. (L 167) 10, 17–18 [hereinafter EUCD].

282. LESSIG, *supra* note 242, at 127; s*ee also Digital Rights and Wrongs*, ECONOMIST, July 17, 1999, at 76 (describing copy-duty as "the legal obligation of copyright holders to provide public access" to their works).

283. Dusollier, *supra* note 102, at 52.

284. *See id.* at 53.

285. EUCD, *supra* note 281, art. 5(3)(a), 2001 O.J. (L 167) at 16.

ody, are omitted.[286] The EUCD does not oblige copyright holders to guarantee public access to their works for these purposes.[287]

Because of these weaknesses, the EUCD is perhaps more useful as a template or model than as a specific guide for legislative action in the United States. In an innovative feature, the EUCD enlists copyright holders as participants in the process of preserving fair use. Bringing all the interested parties into the process in this fashion is not only practical, but politically shrewd. While increasing the likelihood that whatever technological measure ultimately adopted will be effective, such an inclusive approach also diminishes the resistance that would undoubtedly follow if copyright holders believed that change were being imposed upon them without their participation.

This is not to say that any legislative action in this arena would not stir controversy. Copyright holders probably find the legislative status quo quite satisfactory precisely because it permits them to adopt DRM mechanisms that, in practice, restrict users' ability to use content in ways unsatisfactory to copyright holders, irrespective of fair use rights. Copyright holders may be expected to greet legislative attempts to increase technological protections for fair use with skepticism.

At bottom, however, resistance to consumers' ability to exercise fair use rights is indistinguishable from resistance to fair use itself. There can be no reasoned justification for a legal regime that reduces the fair use section of the Copyright Act to a paper tiger. If United States public policy is to change such that users may not engage in what were previously considered to be fair uses of copyrighted works, candor and the due process principle of notice demand that Congress say so openly, rather than allowing the DMCA's anti-circumvention provision to tacitly swallow the fair use statute as more and more copyrighted works are issued in DRM-protected form. The public debate over the proper balance of interests in copyright law that would flow from an initiative to strengthen technological protections for fair use would itself be welcome.[288]

---

286. *See* Dusollier, *supra* note 102, at 53.

287. For a discussion of a number of lingering issues in the interpretation of the EUCD and in the parallel enabling legislation of many EU member nations, see Urs Gasser & Michael Girsberger, *Transposing the Copyright Directive: Legal Protection of Technological Measures in EU-Member States: A Genie Stuck in the Bottle?*, Berkman Publication Series No. 2004-10, at 10–11, 17–24 (Nov. 2004), http://cyber.law.harvard.edu/media/files/eucd.pdf.

288. *See* FISHER, *supra* note 4, at 119 (lamenting that questionable court decisions in peer-to-peer file-sharing cases short-circuited the useful democratic debate that would have resulted from leaving the issues for resolution by Congress); *see also* LESSIG, *supra* note 246, at 199–207 (advocating the necessity of a public, democratic reaction to the specter of the criminalization of massive numbers of American copyright violators).

VI. CONCLUSION

If DRM, in one form or another, is truly here to stay, there is a vital public interest at stake in the form that DRM ultimately takes. Differing DRM designs strike differing balances between the protections conferred on users and content providers; the choice of which balance is the "right" one has far-reaching ramifications for both parties. The issue merits discussion. So far, however, the discussion has been a monologue. Only the voices of copyright holders have perceptibly influenced the design and implementation of DRM technologies and legal protections against circumvention. The technologies that have resulted, perhaps unsurprisingly, reflect not a balancing of interests, but the interests of large content producers alone.

The more technology reflects only one set of interests, however, the more it departs from the law, which conceptualizes copyright as a balancing of interests, with the ultimate goal of fostering both creative expression and broad public availability of creative works. The result has been a perverse scenario nowhere commanded by the Copyright Act or the DMCA, in which technological measures have been allowed to override the fair use doctrine. The daily experience of users departs from existing law, and the public has never been offered any explanation why fair use should mean something different (and far less) in the digital domain than in the offline world. As a result, users have responded by attempting to use copyrighted digital works in the manner they always have, and chafing at the technological limitations that prevent them from doing so.

This situation is neither desirable nor stable. Neither, however, is it inevitable. If a DRM mechanism is engineered to protect the process by which users exercise their fair use rights, their experiences will more closely approach what they are accustomed to in the offline world. Such a system would permit users to assert their statutory rights to engage in fair uses of DRM-protected works, subject to the deterrence of abuse through an (initially anonymous) audit trail. By recognizing and accommodating the rights of parties on both sides of the fair use equation, such an implementation might well be the first system of "digital rights management" truly worthy of the name.