Draft 8/18/00. Please do not cite or quote without permission.

FAIR USE INFRASTRUCTURE FOR COPYRIGHT MANAGEMENT SYSTEMS

DAN L. BURK* & JULIE E. COHEN**

INTRODUCTION

Rights management systems and laws designed to protect these systems from circumvention occupy an increasingly central role in increasingly heated discussions about online copyright enforcement. Proponents argue that without these systems and laws, there is no possibility of meaningful copyright enforcement online. Opponents contend that the emerging technical and legal regimes for digital rights management threaten copyright's traditional balance of rights and limitations, and are inconsistent with the preservation and growth of a vibrant public domain. Without abandoning the views we have previously stated on those matters, we would like to ask some rather different questions. Thus far, the debate about rights management systems has taken them as given. We would like to question this assumption. Can rights management systems be designed and implemented in a way that preserves fair use? If so, how might the law encourage this? Should the law do so?

In this paper, we consider whether rights management systems can be supported by legal and institutional infrastructures that enable appropriate access to the works secured by these technologies. We begin in Part I by reviewing the contours of the fair use doctrine and the legal and policy requirements that mandate appropriate public access to copyrighted works and other publicly available informational works. Part II discusses the nature and purpose of copyright management systems, their legal status under the current anti-circumvention provisions of U.S. law, and their likely effects on fair use. In Part III we consider the foreseeable technical and institutional options that might enable proper public access to secured works and offer a proposal combining minimum system flexibility requirements in exchange for copyright enforcement and "key escrow" in exchange for anti-circumvention protection. Part IV assesses the legal feasibility of such a system, and concludes that the proposal comports with the

---

* Professor of Law & Vance K. Opperman Research Scholar, University of Minnesota.

** Associate Professor of Law, Georgetown University Law Center. We would like to thank the University of Minnesota Law School and The Georgetown University Law Center for summer research funding, and Kathleen Howard (University of Minnesota) and Mitzi Chang and Ilana Safer (Georgetown) for their excellent research assistance.

United States' obligations under international copyright agreements. Finally, Part V considers whether implementation of a key escrow infrastructure for fair use would represent good policy.

I. THE SOCIAL FUNCTIONS OF FAIR USE

Fair use performs a variety of related functions within the policy framework of copyright law. First, the Supreme Court has identified fair use as a type of "safety valve" between the purposes of copyright and the demands of the First Amendment.[1] Copyright clearly constitutes a type of restraint on speech; the author's property right in an expressive work legally restrains others in their use of that expression. Such governmental restraints on speech are typically disfavored; yet in the case of copyright, the Constitution both allows copyright restrictions and disallows governmental interference with free expression. Fair use mediates between these apparently contradictory constitutional provisions by allowing the use of otherwise protected material in criticism, comment, parody, news reporting, and similar uses in the public interest. This arrangement preserves property rights in creative works while allowing sufficient public access to accommodate the public interest in open dialogue and social discussion.

Fair use has also been identified as a device for correcting two types of market failure that are likely to occur in the market for propertized information created by the Copyright Act.[2] On a theory of "market failure," fair use exists to facilitate worthwhile uses of copyrighted works in instances where the value of the use is exceeded by the transaction costs of negotiating a license. Under such conditions, an unfettered right to exclude might deter such valuable uses: the potential user of the work is unlikely to expend more to locate the owner and negotiate a license than he can recover from the licensed use. The fair use doctrine allows the potential user to take the needed portion of the work and make use of it without seeking a license, bypassing the need for deterrent high-cost authorization.

But the unadorned market failure theory cannot by itself explain or justify much of the jurisprudence of fair use. This theory would justify fair use under conditions of low transaction cost only for unauthorized uses of relatively minor value, and for more substantial unauthorized uses only where the transaction costs were exceptionally high. Yet the Supreme Court has made clear that unauthorized use

---

[1] *See* Harper & Row v. Nation Enters., 471 U.S. 539, 556 (1985).

[2] Wendy Gordon, *Fair Use as Market Failure: A Structural and Economic Analysis of the Betamax Case and its Predecessors*, 82 COLUM. L. REV. 1600 (1982).

of a work may be fair even when the copyright owner can be easily located and licensing mechanisms are available. For example, in *Campbell v. Acuff-Rose*,[3] the Court held that unauthorized adaptation of a copyrighted song for parody by the rap music group 2 Live Crew might qualify as fair use, even though 2 Live Crew had requested, and been refused, a license.[4] Additionally, the 2 Live Crew parody was marketed for profit, which suggests that the value of the use to the group outweighed the transaction costs of licensing – indeed quite the opposite value differential seems likely.

The 2 Live Crew case thus is emblematic of a second type of "fair use" market failure in which the value of socially beneficial uses of copyrighted works is not fully internalized.[5] Commentary, criticism, parody, and other unauthorized uses may be of significant value in stimulating public debate and fostering an informed populace, but this value is diffuse, and accrues to recipients other than the user of the copyrighted work.[6] A certain amount of unregulated private noncommercial sharing and copying of works also generates substantial but diffuse value, by fueling serendipitous creation and facilitating the free flow of ideas within society.[7] Where such positive externalities are present, social welfare would be increased by the use of the work, but the potential user may deterred from doing so because he will not assess the use by its full value. In such cases, fair use may again serve to bypass licensing that appears excessively high-cost from the perspective of the potential user.[8] Because of the subject matter of

---

[3] 510 U.S. 569 (1994).

[4] *Id.* at 594.

[5] *See* Robert P. Merges, *Are You Making Fun of Me?: Notes on Market Failure and the Parody Defense in Copyright*, 21 AIPLA Q.J. 305 (1993).

[6] *See* Julie E. Cohen, Lochner *in Cyberspace: The New Economic Orthodoxy of "Rights Management"*, 97 MICH. L. REV. 462 (1998); Lydia Pallas Loren, *Redefining the Market Failure Approach to Fair Use in and Era of Copyright Permission Systems*, J. INTELL. PROP. L. 1 (1997). Alfred Yen has argued that society may also have "non-economic" interests in the production of such uses. *See* Alfred C. Yen, *When Authors Won't Sell: Parody, Fair Use, and Efficiency in Copyright Law*, 62 COLO. L. REV. 79 (1991); *see also* Cohen, *supra*, at 551-59.

[7] Although few litigated cases have involved private noncommercial defendants, the Supreme Court's decision in Sony Corp. of Am. v. Universal City Studios, Inc., 464 U.S. 417 (1984), makes clear that even widespread private noncommercial copying may be fair. *See id*. at 447.

[8] This problem reaches its zenith in cases of critical review or parody that might damage the market for the underlying work: society has a strong interest in the commentary or the burlesque, but the production of such a derivative work is directly contrary to the interests of the owner of the criticized. *See Campbell*, 510 U.S. at 590-92; Richard A. Posner, *When is Parody Fair Use?*, 21 J.LEGAL STUD. 67 (1992).

copyright, instances of such positive externality will tend to track the social purposes of the First Amendment: broader dissemination of literary, artistic, and similar works will tend directly or indirectly to sustain social dialogue and public debate. Thus, fair use may accommodate free speech interests directly, by providing the content for such exchanges, and indirectly by fostering an aware and educated populace better able to participate in both public debate and the creation of future works of authorship.

Finally, fair use ensures the development of new markets in copyrightable works where copyright holders might otherwise dominate or impede such development. For example, in an extensive line of cases dealing with computer software development, courts have used fair use to provide "breathing room" for the reverse engineering of copyrighted programs.[9] The creation of software complementary to a given computer program may require examination of that program's structure in order to design an interoperable product. Unless patented, the utilitarian functions of computer programs lie in the public domain and may be freely copied by firms developing competing or complementary products. But examination of software through decompilation of the code necessarily creates a copy of the program being studied. This copying during the process of reverse engineering might be considered an infringement of the copyright in the program studied. However, courts have consistently held that making temporary or intermediate copies in order to study the program and extract its public domain information is fair. Thus fair use serves as a mechanism to preserve a right of reverse engineering, maintaining access to the uncopyrighted or public domain elements of the programs that may be incorporated into new products.

In a related application, fair use catalyzes limitations on the reach of contributory liability, allowing development of markets ancillary to those for copyrightable works. Under U.S. law, provision of a technology or service that facilitates copyright infringement may itself constitute infringement. But such contributory infringement occurs only when the technology provided to enable direct infringement has no substantial non-infringing use – in other words, when the device supplied has essentially no use other than to infringe.[10] This shelter for "dual purpose" technologies prevents copyright holders from stunting the

---

[9] *See* Sony Computer Entertainment Corp. v. Connectix, 203 F.3d 596, 602-08 (9th Cir. 2000); DSC Communications Corp. v. DGI Technologies, 81 F.3d 597, 601 (5th Cir. 1996); Bateman v. Mnemonics, Inc., 79 F.3d 1532, 1539 n.18 (11th Cir. 1995); Sega Enters., Ltd. v. Accolade, 977 F.2d 1510, 1520 (9th Cir. 1992); Atari Games Corp. v. Nintendo of Am., 975 F.2d 832, 843-44 (Fed. Cir. 1992).

[10] *See* Sony Corp. of Am. v. Universal City Studios, Inc., 464 U.S. 417, 442 (1984).

development of new markets tangential to existing proprietary interests, which might otherwise be dominated or stifled by overbroad application of contributory liability.

Fair use will frequently provide the permissible application needed invoke protection for "dual purpose" technologies and their associated products. For example, in the most famous iteration of the substantial non-infringing use standard, *Sony v. Universal Studios*,[11] the Supreme Court held that sale of the Sony Betamax video recorder was not contributory infringement, despite the device's capacity to facilitate infringing recording of broadcast audiovisual works. The necessary non-infringing use was found in the practice of "time shifting," that is, taping a televised show at one time to be viewed at a later time, which the court found to be a fair use. This holding cleared the path for a flourishing market in home video recorders, and concomitant development of a lucrative market for sale and rental of the plaintiff industry's audiovisual works.[12]

In sum, fair use plays an important – and constitutionally-required – role in the dissemination and production of cultural products. As we now describe, however, fair use is currently threatened by a combination of new distribution technologies and unreflective legislative action.

II. CURRENT TECHNICAL AND LEGAL INFRASTRUCTURES FOR RIGHTS MANAGEMENT

For copyright owners, digital networks represent both a promise and a threat. Computer networks eliminate or minimize many of the costs associated with the publication and distribution of information products, but also substantially eliminate the costs of making and distributing unauthorized copies. Although scholars and industry commentators have disputed predictions that digital networks will destroy the market for authorized copies of works, copyright owners have stated a reluctance to

---

[11] *See id*.

[12] Several commentators have highlighted what they see as the irony of a ruling that permitted content users to profit handsomely by losing their infringement claim. But this supposition flies far of the mark. Had the Court held provision of VCRs to be contributory infringement, we might still expect the market for video recorders and video rentals to emerge. A holding in Universal's favor would be equivalent to granting a property right to exclude VCR manufacturers from selling their devices. Under a Coasean theory of arbitrage, assuming manageable transaction costs, if there were money to be made from the sale of VCRs, one would expect home electronics manufacturers to negotiate a license from the copyright holders. Thus the issue is not so much whether consumers would gain access to VCRs, and so whether the market for video rentals would develop, as who would control the development of that market.

experiment with digital distribution without additional legal and technological protection against unauthorized copying.[13] Within the past few years, they have succeeded on both fronts. These legal and technological protections confer a degree of control over access to and use of copyrighted content that goes well beyond the rights afforded by copyright law.

Together with technology experts, the copyright industries have developed secure packaging and delivery software designed to prevent purchasers and third parties from making unauthorized uses of digital works. As envisioned by the copyright industries, these "rights management systems" will be capable of controlling, monitoring and metering almost every conceivable use of a digital work.[14] This increased control, however, will allow copyright owners to appropriate far more protection than copyright law now provides. Of particular significance for this paper, copyright law allows some reuse of protected expression under the fair use doctrine (and also under a variety of other exceptions designed to serve the public interest), and allows any reuse after the term of copyright protection has expired.[15] Rights management systems, in contrast, can insist that permission be sought, and a fee paid, for any reuse.

---

[13] *See, e.g.*, *WIPO Copyright Treaties Implementation Act: Hearing on H.R. 2281 Before the Subcomm. on Telecommunications Trade & Consumer Protection of the House Comm. on Commerce*, 105th Cong. (1998) (statement of Robert W. Holleyman, II, President, The Business Software Alliance); *Copyright Legislation: Hearings on H.R. 2281 Before the Subcomm. on Cts. & Intell. Prop. of the House Comm. on the Judiciary*, 105th Cong. (1997) (statements of Robert W. Holleyman, II, President, The Business Software Alliance; Allee Willis, on behalf of Broadcast Music, Inc.; Tom Ryan, CEO, SciTech Software, Inc., on behalf of the Software Publishers' Association; Gail Markels, General Counsel and Senior Vice President, Interactive Digital Software Association; and Allen R. Adler, Vice President for Legal and Governmental Affairs, Association of American Publishers); *National Information Infrastructure: Hearing on S. 1284 Before the Senate Comm. on the Judiciary*, 104th Cong. (1996) (statement of Kenneth R. Kay, Executive Director, Creative Incentive Coalition); *Copyright Protection on the Internet: Hearings on H.R. 2441 Before the Subcomm. on Cts. & Intell. Prop. of the House Comm. on the Judiciary*, 104th Cong. (1996) (statements of Barbara A. Munder, Senior Vice President, The McGraw-Hill Companies, Inc.; Frances W. Preston, President and CEO, Broadcast Music, Inc.; Jack Valenti, Chairman and CEO, Motion Picture Association of America, Inc.; and the Association of American Publishers).

[14] *See, e.g.*, Daniel J. Gervais, *Electronic Rights Management and Digital Identifier Systems*, J. ELECTRONIC PUBLISHING, March 1999, <http://www.press.umich.edu/jep/04-03/gervais.html>; IPR Systems, *What is Rights Management: The Nature of Knowledge and Rights Management Systems*, <http://www.iprsystems.com/html/rights_management.html>; Mark Stefik, *Shifting the Possible: How Digital Property Rights Challenge Us to Rethink Digital Publishing*, 12 BERKELEY TECH. L.J. 138 (1997). For useful directories of entities currently conducting rights management research and/or offering rights management services, see Gervais, *supra*; Lock-My-Doc, *Digital Rights Management (DRM)*, <http://www.lockmydoc.com/drm/drm.html>.

[15] *See, e.g.*, 17 U.S.C. §§ 108 (library copying privileges), 109(a) (limitation of exclusive distribution right to first sale of copy for most works), 110 (public performance and display exemptions for nonprofit activities and organizations); *see also id.* § 302 (establishing duration of copyright protection).

The copyright industries also have succeeded in obtaining extremely broad legal protection for rights management systems. After nearly three years of lobbying, both in Congress and in international treaty proceedings, the copyright industries were rewarded with Title I of the Digital Millennium Copyright Act (DMCA), which prohibits tampering with or circumvention of these systems, and also prohibits the manufacture, distribution, and importation of circumvention tools.[16] The DMCA also authorizes the Librarian of Congress, in consultation with the Register of Copyrights, to assess the impact of the circumvention ban on traditional fair use practices and, if necessary, to issue rules exempting certain users of certain categories of works from the ban.[17] The statute clearly states, however, that any such exemptions will not afford a defense to the prohibition on circumvention technologies.[18] As a practical matter, therefore, any exemptions ultimately declared will have very limited utility; self-evidently, most users will be unable to exercise their circumvention rights unless they are provided with the tools to do so.

The development of rights management systems graphically demonstrates the power of technology to supplement and even supplant legal regulation. Much as physical barriers and spatial relations constrain behavior in actual space, technical standards constrain behavior in cyberspace. In the physical world, people cannot walk through solid walls, occupy two spaces simultaneously, or carry skyscrapers away in their pockets. Similarly, there are certain activities that simply cannot be performed on a particular computer system, because the system is not built to accommodate the behavior – the system may be programmed to deny access without a password, prevent logging on simultaneously from two terminals, or prohibit alteration of a file that is designated "read only."

This observation that the technology will only do what the technology will do at first consideration may seem blatantly obvious, and even tautological. But as Larry Lessig and Joel Reidenberg have pointed out, technical standards are within the control of the designer, and so confer upon the designer the power

---

[16] Digital Millennium Copyright Act, Pub. L. No. 105-304, Title I, 112 Stat. 2860 (1998), *codified at* 17 U.S.C. § 1201(a)-(b). The 1996 WIPO Copyright Treaty and its requirements concerning legal protection for rights management systems are discussed in Part IV, *infra*.

[17] 17 U.S.C. § 1201(a)(1)(B)-(D).

[18] 17 U.S.C. § 1201(a)(1)(E).

to govern behavior with regard to that system.[19] By consciously building constraints on behavior into the technical standards governing a technology, the technical standards effectively become a new method for governing behavior vis a vis that technology – in essence, the technical standards become a type of law. Such technical rule sets may supplement or even supplant the legal rule sets designed to govern such behavior. Government may choose to employ or enforce technical standards to achieve goals that might otherwise be achieved by legal rulemaking. Reidenberg in particular has examined in detail the complex set of interactions that he dubs "lex informatica," by which governmental action can shape technological standards into a substitute for legal controls.[20]

The design of technological constraints, however, is not the sole provenance of the state; indeed, it is more often left to private parties. In the case of rights management systems, copyright owners determine the rules that are embedded into the technological controls. By implementing technical constraints on access to and use of digital information, a copyright owner can effectively supersede the rules of intellectual property law. For example, as described above, it may decide that the technological controls will not permit any copying of the controlled content, whether or not the copying would be fair use.[21] If the integrity of the controls is backed by the state, as it is under the DMCA's anti-circumvention provisions, the result is to shift enforcement of the rights-holder's interest from penalties for unauthorized infringement to penalties for unauthorized access.

The implications of this development are stark: Where technological constraints substitute for legal constraints, control over the design of information rights is shifted into the hands of private parties, who may or may not honor the public policies that animate public access doctrines such as fair use. Rights-holders can effectively write their own intellectual property statute in computer code. Moreover, to the extent that the DMCA appears to legitimate technological controls over copyrighted works, without regard to their effect on public policy, the statute effectively grants rubber-stamp approval to such private

---

[19] LAWRENCE LESSIG, CODE AND OTHER LAWS OF CYBERSPACE (1999); Joel R. Reidenberg, *Lex Informatica*, 76 TEX. L. REV. 553 (1998).

[20] *See* Reidenberg, *supra* note __, at 568-76.

[21] *See* Stefik, *supra* note __, at 147.

legislation. Yet this result – allowing every copyright owner to custom-design its own version of copyright law – cannot conceivably have been what Congress intended.[22]

Of course, the promulgation of technologically embedded rule sets is not the first situation in which private allocation of rights information has been encouraged and enforced by public institutions. Most notably, the coercive power of the state is routinely brought to bear in the case of contractual agreements, which may include confidentiality agreements, intellectual property licenses, or other private informational access allocations. Since technical controls can impose conditions that might formerly have been the subject of a detailed license agreement, such controls might be viewed as equivalent to a sort of licensing regime. (In addition, access to technologically controlled information also may be conditioned upon acceptance of a given set of licensing provisions governing the type and frequency of usage.) Then (extending the analogy), penalties for circumvention of the technological constraints simply stand in for the private law of contract, which penalizes breach of license.

But such a comparison to contract law by no means justifies employment of technical controls that contravene the established public policy of copyright. Where traditional contracts are at issue, carte blanche enforcement of private agreements has never been the rule in Anglo-American law. When such agreements are found illegal, unconscionable, or simply in violation of public policy, they are held unenforceable.[23] Because contract law is state law, a similar result also may be reached on grounds of federalism: where enforcement of a state law contract would violate the public policy inherent in the federal intellectual property scheme, or that embedded in the Constitution itself, such contractual provisions are preempted.[24] Attempts to leverage the statutory right via contracts extending beyond the limits intended by Congress, or authorized by the Constitution, constitutes grounds for voiding the contract.

---

[22] Other language in the DMCA indicates as much. *See* 17 U.S.C. § 1201(c)(1).

[23] *See* RESTATEMENT (2D) OF CONTRACTS §§ 8, 178, 179, 208 (1979).

[24] For detailed analysis of the preemption question, see Julie E. Cohen, *Copyright and the Jurisprudence of Self-Help*, 13 BERKELEY TECH. L.J. 1089, 1129-33 (1998); David L. Lange, *The Intellectual Property Clause in Contemporary Trademark Law: An Appreciation of Two Recent Essays and Some Thoughts About Why We Ought to Care*, 59 LAW & CONTEMP. PROBS. 213 (1996); David Nimmer, Elliot Brown, & Gary N. Frischling, *The Metamorphosis of Contract Into Expand*, 87 CALIF. L. REV. 17 (1999); Malla Pollack, *Unconstitutional Incontestability? The Intersection of the Intellectual Property and Commerce Clauses of the Constitution: Beyond a Critique of* Shakespeare Co. v. Silstar Corp., 18 SEATTLE U. L. REV. 259 (1995).

There is no reason to suppose that this result should differ for technological analogues to contracts. Where rights management systems attempt to impose restrictions on informational content that would be prohibited in a contractual agreement, the restrictions should be viewed as equally repugnant to public policy and equally void. One of us has previously argued that the coercive power of the state should be extended in support of technological constraints no farther than it may be to enforce statutory or contractual constraints.[25] Further, where the Constitution imposes limitations upon the government's creation of property rights, those limitations apply equally to both legally and technologically delineated property. In some instances of overreaching via technological controls, the Constitution may even demand a limited self-help right, or "right to hack," to surmount privately erected technological barriers to information that the Constitution requires be publicly accessible.[26]

The familiar reply from the proponents of the anti-circumvention provisions appeals not to the language of contract, but to the legitimate right to control access to private property. There is no right, it has been said, to break and enter a dwelling in order to gain access to public domain information.[27] This analogy to tangible property concludes that deployment of management systems to control access to intellectual property is no different than fencing or walling off privately held real estate. This analogy is highly problematic even in concept; both the economics of intangible information and the scope of state-granted rights in informational works differ markedly from the economic and legal bases for private rights in real property. But even to the extent that an analogy to real property may hold true, the argument proves too much. The owner of private real estate cannot legitimately fence off easements or public rights of way, or extend the fence to encompass public thoroughfares.[28]

Indeed, if the real property analogy is to be followed, public rights of access have long trumped the private right to fence. On a real property analogy, CMS "fencing" finds a close parallel in the nineteenth-century enclosure of private land using the newly developed fencing technology of barbed

---

[25] Cohen, *Self-Help*, *supra* note __, at 1140-42.

[26] *See id*. at 1140-42.

[27] *See, e.g.*, David Friedman, *In Defense of Private Orderings*, 13 BERKELEY TECH. L.J. 1151 (1998), Raymond T. Nimmer, *The Relation Between Contract and Intellectual Property Law*, 13 BERKELEY TECH. L.J. 827 (1998).

[28] *See* 43 U.S.C. §§ 1061, 1063; Camfield v. United States, 167 U.S. 528 (1897); Stoddard v. United States, 214 F. 566 (8th Cir. 1914); Hanley v. United States, 186 F. 711 (9th Cir. 1911).

wire. The application of this technology to open lands led the infamous "range wars," in which fencing of previously accessible parcels of privately owned range was countered by illegal fence-cutting tactics. But it is important to note that the development of this cheap and effective means of fencing prompted not only enclosure of legitimately held private lands, but also illegitimate and unauthorized enclosure of *public* lands. The end result was the enactment of statutes that penalized *both* cutting of legitimate fences enclosing private property *and* the unauthorized enclosure of public lands.[29]

The anti-circumvention provisions of the DMCA may to some extent be viewed as responses to the threat of "fence-cutting," that is, hacking around rights management systems implemented by copyright owners. But the analogy is more complete: the use of technology to block public access to public domain elements of managed content parallels the unauthorized fencing of public lands. Unlike nineteenth-century fence-cutting laws, however, the anti-circumvention provisions do nothing to ensure that the public continues to enjoy fair use "easements" or "rights of way" that copyright holders have no legitimate right to withdraw from public access. This cannot be because such public rights no longer are recognized; the current text of the DMCA gives no indication of having repealed or annulled such public access rights. To the contrary, the statute explicitly states that fair use continues to inure in digital media.[30] Yet the current language of the statute makes no provision for such access.

The question then, as one commentator has aptly observed, is whether in its reaffirmation of fair use, Congress has simply made an empty promise.[31] There is no need for it to be. As Reidenberg in particular has shown, Congress has at its disposal a variety of possible tools for directing technological development into channels that will further established public policy goals.[32] We suggest that in the case of copyright management systems, this order has been disastrously inverted: perceived technological imperatives are improperly driving the enactment of legal prohibitions. The rapid development and spread of technologies for digital copying and distribution has prompted a rush to legally shore up technological

---

[29] *See* 43 U.S.C. §§ 1061, 1063; ERNEST STAPLES OSGOOD, THE DAY OF THE CATTLEMAN 191-95 (1929); Scott S. Smith, *The Wire that Won the West*, AM. HERITAGE INVENTION & TECH., Fall 1998, at 34, 38-40.

[30] *See* 17 U.S.C. § 1201(c)(1).

[31] *See* Pamela Samuelson, , *Intellectual Property and the Digital Economy: Why the Anti-Circumvention Regulations Need to Be Revised*, 14 BERKELEY TECH. L.J. 519, 546-47 (1999)

[32] *See* Reidenberg, *supra* note __, at 586-92.

safeguards against such copying, without proper consideration of the policy balance that should animate the legal and technical infrastructure. Instead, legal protections for rights management systems should be designed with the desired policy balance in mind. Next, we consider various possible mechanisms for achieving that result.

III. OPTIONS FOR FAIR USE INFRASTRUCTURE

Currently, the DMCA's anti-circumvention provisions effectively sanction the use of private code to write the public law of fair use out of existence. But the legal regime governing rights management technologies need not be structured in such a fashion. Instead, law may equally well be designed to shift technological development in a direction that balances the incentive structure of copyright protection with copyright's concern for the public domain and for the legitimate fair use privileges of the public. Here, we suggest modifications to the DMCA designed to create incentives for the preservation of fair use in digital media.

Realizing the promise of fair use in a digital rights management environment will require some technical mechanism to allow public access and reuse privileges equivalent to those deemed fair in previous media. In broad brush, there are two ways that such a system might be designed. First, the rights management system itself might be designed to detect and regulate fair use access. Second, a decisionmaker external to the rights management system might authorize would-be fair users to override rights management controls.

A. Coding for Fair Use

The most direct method of accommodating fair use would be to mandate or prompt the development of rights management systems that directly allow purchasers of a work to make fair use of the content. Optimally, the "breathing space" required for fair uses would be programmed directly into the technical rule set that controls access to the work. The systems might, for example, include provisions allowing users to extract a certain number of bits, or display the work for certain periods of time, or partially perform the work a certain number of times. Depending on the characteristics of the desired use, users would be able to take these actions without having to seek additional permission or pay additional fees.

In reality, however, an algorithm-based approach to fair use is unlikely to accommodate even the shadow of fair use as formulated in current copyright law. We are not optimistic that system designers will be able to anticipate the range of access privileges that may be appropriate in order for fair uses to be made of a particular work. Neither are we optimistic that system designers will be able to anticipate the types of uses that would be considered fair by a court. Fair use is irreducibly a situation-specific determination. In some instances, a user may fairly take a work in its entirety – say, for example, where the work is entitled to only thin protection, the use is for a protected use such as scholarship or criticism, and/or the use is expected to have no appreciable impact on the market for the work.[33] In other situations, where three or four of the factors weigh heavily against a particular use, taking much less might exceed fair use.[34] Building the range of possible 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, meaning that (at least for now) there is no feasible way to build rights management code that approximates the results of judicial determinations.

An alternative might be for copyright holders to build into rights management systems some level of discretionary access for users that would fall within a range that would almost always constitute fair use, or that at least would fall within a range of use that the copyright holder would be unwilling to contest was fair. In the past, some attempts have been made to set similar standards, as for example in the case of the so-called "safe harbor" provisions for educational photocopying negotiated by the educational and copyright content interests during the 1976 revisions to the Copyright Act, or in the case of the aborted "Conference on Fair Use" (CONFU), which attempted to negotiate fair use standards for digital and multimedia works.[35] Such default parameters for fair use represent private agreements by stakeholders

---

[33] *See, e.g.*, Campbell v. Acuff-Rose, 510 U.S. 569 (1994); Sony Corp. of Am. v. Universal City Studios, Inc., 464 U.S. 417 (1984); Sega Enters. v. Accolade, 977 F.2d 1510 (9th Cir. 1992); Higgins v. Detroit Education Television Foundation, 4 F. Supp. 2d 701, 707 (E.D. Mich. 1998).

[34] *See, e.g.*, Harper & Row Publishers, Inc. v. Nation Enterprises, 471 U.S. 539, 564 (1985); Nihon Keizai Shimbun, Inc. v. Comline Business Data, Inc., 166 F.3d 65, 72 (2d Cir. 1999).

[35] *See* H.R. REP. NO. 94-1476, 94th Cong., 2d Sess., at 68-74 (1976) (setting forth Agreement on Guidelines for Classroom Copying in Not-for-Profit Educational Institutions With Respect to Books and Periodicals), *reprinted in* 1976 U.S.C.C.A.N. 5659, 5681-88; INFORMATION INFRASTRUCTURE TASK FORCE, INTELLECTUAL PROPERTY AND THE NATIONAL INFORMATION INFRASTRUCTURE: THE REPORT OF THE WORKING GROUP ON INTELLECTUAL PROPERTY RIGHTS 83-84 (1995) (discussing establishment and progress of CONFU) [hereinafter "NII WHITE PAPER"].

to treat the designated level of usage as fair use, without a prior judicial determination. Such agreed-upon standards might be built into the access permitted by rights management systems.

However, we are again skeptical about the ability of negotiated defaults to capture the full range of social benefit that more flexible legal standards allow. While these defaults sometimes might allow access that would exceed fair use under a judicial determination, the "safe harbor" concept is more likely to tend toward a minimalist view of fair use. We suspect that copyright holders would be willing to concede fair use in only a small fraction of the situations that would constitute fair use – indeed, it was just such insistence upon minimalist guidelines by rights holders that led to the collapse of the CONFU discussions.[36] Moreover, in the case of the 1976 "safe harbor" guidelines for educational copying, rights holders, content users, and even courts have shown a deplorable tendency to act as though the guidelines defined the outer limits of fair use.[37] To the contrary, such guidelines were intended to delineate fair use minima: a floor rather than a ceiling.[38] We are consequently reluctant to recommend an infrastructure based solely on the design of similar defaults into self-enforcing "lock-out" systems for fear that the "ceiling" effect could be even more pernicious.

A variant on the concept of directly designed fair use "defaults" looks to a slightly different source. Judicial determinations and negotiated minimum standards are not the only possible measures of current fair use practice; arguably, the more accurate measure of fair use is the daily behavior of ordinary users.[39] Rather than approximating the results of fair use jurisprudence or the products of interest-group

---

[36] *See Final Report to the Commissioner on the Conclusion of the Conference on Fair Use* (Nov. 1998), <http://www.uspto.gov/web/offices/dcom/olia/confu/index.html> (visited Aug. 16, 2000).

[37] *See, e.g.*, Princeton University Press v. Michigan Document Services, Inc., 99 F.3d 1381 (6th Cir. 1996) (en banc), *cert. denied*, 117 S. Ct. 1336 (1997); Basic Books, Inc. v. Kinko's, Graphics Corp., 758 F. Supp. 1522 (S.D.N.Y. 1991); Marcus v. Rowley, 695 F.2d 1171 (9th Cir. 1983); Harper & Row, Publishers v. Tyco Copy Service, Copyright L. Rec. (CCH) ¶ 25,230 (D. Conn. 1981); Basic Books, Inc. v. Gnomon Corp., Copyright L. Dec. (CCH) ¶ 925,145 (D. Conn. 1980); NII WHITE PAPER, *supra* note __, at 82-83 ("Educational uses that serve the same ends and are constrained in the same manner as the copying permitted under the Classroom Guidelines will likely be fair. . . ."); Robert Kasunic, *Fair Use and the Educator's Right to Photocopy Copyrighted Material for Classroom Use*, 19 J. COLL. & UNIV. L. 271, 281, 284-85 (1993); Albert D. Spaulding, *Fair Use of Research and Course Packets in the Classroom*, 31 AM. BUS. L.J. 447, 448 (1993).

[38] *See* H.R. REP. NO. 94-1476, 94th Cong., 2d Sess., at 59 (1976), *reprinted in* 1976 U.S.C.C.A.N. 5659, 5718

[39] *Cf.* Jessica Litman, *The Exclusive Right to Read*, 13 CARDOZO ARTS & ENT. L.J. 29, 35-37 (1994); Jessica Litman, *Copyright Noncompliance (or Why We Can't "Just Say Yes" to Licensing)*, 29 N.Y.U. J. INT'L L. & POL'Y 237 (1997).

bargaining, rights management systems might be designed to approximate fair use norms. For this to work, copyright management systems would need to sanction a large amount of unauthorized copying, but on a relatively small scale.[40] A precedent for this sort of rule is the Audio Home Recording Act, which requires that digital audio tape recordings and recording devices be designed to accommodate serial copy management technology that allows the production of only one generation of perfect copies.[41]

Norm-based fair use defaults, however, are subject to many of the same criticisms as negotiated fair use defaults. Because programmed defaults, however derived, are still inflexible at the margin, they cannot encompass the full range of uses that a court would hold fair. Thus, if norm-based controls are regarded as implementing a fair use ceiling rather than a fair use floor, users of digital works will enjoy far less fair use than they have enjoyed in traditional media. 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. Once again, we cannot recommend a fair use infrastructure based solely on this sort of fair use default.

B. Key Access for Fair Use

The second option for the design of fair use infrastructure involves the introduction of an external decisionmaker into the process for obtaining access to technologically secured works. At present, only human intelligence, reviewing the unique circumstances of a particular use, can determine whether it is likely to be fair. Thus, we might require users to apply for keys to access the encrypted work. This option would allow case-by-case determination of the need for access, thus building in judgment capabilities that cannot practically be emulated by technical defaults.

One such method might be to place the fair use determination in the rights holder's hands. We cannot, however, recommend a legal rule that would fundamentally shift the decisionmaking authority about whether to proceed with a use from users to owners. As we have described above, fair use frequently condones public access in situations where the collective public interest runs contrary to the

---

[40] We note that the norm regarding personal copying of music has shifted somewhat with the advent of MP3 compression technology. Whether the law should sanction this shift, and under what circumstances, are hotly contested questions. *See* A&M Records, Inc. v. Napster, Inc., 2000 WL 1009483 (N.D. Cal. July 26, 2000); UMG Recordings, Inc. v. MP3.com, Inc., 92 F. Supp. 2d 349 (S.D.N.Y. 2000). In any process to specify automatic fair use defaults, questions like this will require careful consideration.

[41] *See* 17 U.S.C. § 1002.

rights holder's individual interest. Thus, there may be a strong incentive for the rights holder to deny access just when the public interest most demands access. Currently, users need apply to no one in order to engage in a use the user deems fair, the user simply must be willing to pay infringement damages should her determination be erroneous. Placing the burden of application on the user would drastically change the dynamics of fair use, and would create unacceptable social costs.[42]

In addition, a preauthorization system for fair use is vulnerable to three more general objections. The first and second, closely related, are that a preauthorization requirement would be costly, and would chill spontaneous uses. Case by case determination of the fairness of the intended use would require a lengthy and complicated approval process. But even a quick and inexpensive prescreening procedure will impose some transaction costs, and will deter some uses that otherwise would have been made. As noted above, considerable social benefit accrues from this sort of unplanned use. Research and teaching, in particular, are processes that contain an irreducible element of ad hoc adjustment.

Third, application to a third party is likely to compromise the sort of anonymity that users presently enjoy. Anonymity is the current default for fair use access (and indeed for access generally) in traditional media – a copyright holder does not know who has made use of the work, or at what time, or in what manner. Even if the fair use results in publication or dissemination of a subsidiary work, the author need not reveal her name. For reasons already discussed, we are particularly reluctant to recommend that this situation be inverted by requiring revelation to the rights holder of a user's identity and use for every fair use. More generally, though, there exist a wide range of situations, as for example in the case of a parody or a negative critique, in which the user may prefer to remain anonymous. Requiring parodists or other fair users to apply to for access to any third party may chill such uses. And as one of us has outlined in detail elsewhere, there is a strong case for a constitutional right to receive information anonymously.[43]

---

[42] An example of this sort of burden-shifting is Title II of the DMCA, which establishes a procedure for copyright owners to demand that online service providers remove allegedly infringing material from their systems. *See* 17 U.S.C. § 512(c). In several high-profile disputes, copyright owners have invoked this extrajudicial "notice and takedown" procedure against uses of copyrighted material that lie at the core of protected first amendment activity. *See* Universal City Studios, Inc. v. Reimerdes, 82 F. Supp. 2d 211 (S.D.N.Y. 2000); Julie E. Cohen, *Call it the Digital Millennium* Censorship *Act: Unfair Use*, THE NEW REPUBLIC ONLINE, May 23, 2000, <http://www.tnr.com/online/cohen052300.html> (describing Microsoft's attempt to use the notice and takedown procedure to silence critics of its specification for implementation of the Kerberos Web security standard).

[43] Julie E. Cohen, *A Right to Read Anonymously*, 28 CONN. L. REV. 981 (1996).

Creation of a statutory scheme that requires users to identify themselves would seem to run contrary to this right, and so risks constitutional infirmity.

To avoid the risk of private censorship by rights holders, it seems that any externally-mediated mechanism for preserving fair use in digital works will require the participation of some third party. In some cases, existing institutions might be conscripted into mediating access. For example, one could envision a procedure by which, if the owner had refused access, the needed access could be judicially compelled upon determination that the proposed use was likely to be fair. Something of this sort regularly occurs in patent usage, where declaratory judgments of non-infringement are routinely requested of courts before a plaintiff engages in potentially infringing activity. A legal procedure of this type retains the virtue of avoiding static technical defaults by placing the fair use determination before a human adjudicator, and moreover places the determination back into the hands of a neutral decisionmaker, rather than putting it at the mercy of the copyright holder.

However, a judicially-administered procedure does not seem well calculated to cure cost, spontaneity, or anonymity objections. Any procedure requiring an ex ante evaluation of fairness would dramatically raise the cost of fair use by essentially transforming the fair use right from a liability rule to a property rule. Under the current conception of fair use, the decision whether or not to use a work is made ex ante by the user – if an infringement suit is brought later, the court may or may not validate the user's calculus, but penalties are imposed after the use has been made. Requiring a judicial determination before the use would unquestionably deter many uses. Spontaneous uses would likely disappear altogether. Indeed, under this system, fair use might become the sole provenance of well-capitalized firms with the resources to engage in the process, and which would do so only where the likely reward of gaining access exceeded the cost of the procedure. Moreover, the possibility of anonymous use would again be endangered, absent some procedural device to conceal the identity of the fair use plaintiff during the court proceeding.

External mediation of fair use access thus requires third-party intervention at a relatively low cost, with modifications designed to protect anonymity to the greatest extent possible. This suggests that the mediating party will need to perform functions not currently performed by existing institutions, yet the mediating party still must command the trust of both the owner and the user of the work. Thus, Mark Stefik and Alex Silverman have proposed the idea of a Digital Property Trust, composed of representatives from both the copyright industries and consumer groups, that would administer fair use

access.[44] Their proposal, however, leaves a number of important questions about the operation of such a system unanswered. Recent developments in the law and practice of electronic commerce supply a more detailed model for such a third party institution.

The concept of a trusted third party has become familiar in the context of electronic commerce, where it was determined early on that encryption technology alone could not provide the needed security and authentication for on-line transactions.[45] Public key cryptography can provide technologically unbreakable security, and technologically unfalsifiable user identification, but cannot ensure that the humans who employ the cryptographic keys to the technological systems have kept those keys secure; rather, this technological retrofit of open networks must be supported by institutional infrastructure. Consequently, the intervention of "trusted third parties" has been found necessary to verify the security of keys, and to associate keys with particular users.[46] In order for such institutions to develop, a legal infrastructure clarifying their rights and responsibilities is in turn required. The sum total of this technical, legal, and institutional system has been dubbed public key infrastructure, or PKI.

An analogous situation obtains for the application of encryption to digital rights management. As outlined above, digital media, and most particularly networked media, display the hallmarks of open access: facilitating quick and inexpensive copying of content, as well as the quick and inexpensive distribution of such content. Copyright management systems are to be layered on top of existing protocols in order to close easy access, securing content from copying and distribution, in effect making electronic copies more closely resemble physical copies. But copyright management alone cannot ensure the proper balance of access and security previously achieved in nondigital media.

---

[44] Mark Stefik & Alex Silverman, *The Bit and the Pendulum: Balancing the Interests of Stakeholders in Digital Publishing*, 7 AM. PROGRAMMER 1, 13-14 (1997).

[45] *See* A. Michael Froomkin, *The Essential Role of Trusted Third Parties in Electronic Commerce*, 75 OR. L. REV. 49 (1996). Cryptographic applications have become important to electronic commerce because of the essentially insecure nature of the protocols governing the Internet. This open architecture provides for wide interoperability, and sharing of resources, but does not lend itself to robust security or user authentication. However, with the growth of electronic commerce, the network is increasingly used for purposes that require secure communications and user authentication. To facilitate these new uses, technology based upon public key encryption has been overlaid upon the network to provide security and authentication. *See Public Key Infrastructure Symposium*, 38 JURIMETRICS J. 241 (1998).

[46] *See* Froomkin, *supra* note __.

As in the case of electronic commerce, a new technical, legal, and institutional infrastructure might facilitate the development of trusted third parties to mediate fair use access to technologically protected works. The system we propose hinges upon the concept of key escrow, that is, management of rights management keys by a trusted third party, rather than by the owner of a work. Keys to technologically-protected works would be held by the trusted third party, who would release them to users applying for access to make fair use.

Although, as we have noted, any preauthorization requirement impinges upon spontaneous uses, the trusted third party's approval procedure could be designed to minimize this impact. In order to avoid difficult ex ante judgments about particular uses, and to approximate as nearly as possible the cost and incentive structure of traditional fair uses, the third party would not be required, and would not attempt, to make a determination about the bona fides of the access application. Rather, the third party would simply issue keys to applicants via a simple online procedure.

Solving the anonymity problem is far more difficult. The concept of key escrow has been vilified in the past, and we believe with good reason, when it constituted the core of a governmental plan that would have systematically undermined the integrity of private communications.[47] But a different sort of privacy interest is at stake here, where the issue is public access to publicly distributed works of authorship, rather than governmental access to private communications. In this instance, the concept of third-party escrow works in the public interest and could be made to work in favor of preserving privacy, rather than against both goals.

A trusted third-party system could be designed for true anonymity. Under such a system, the escrow agent would release keys to applicants without retaining or even generating identifying records. Such a system would replicate the anonymity that fair users enjoy in traditional media. In some cases, it might even provide stronger anonymity – as, for example, where access via escrowed keys might substitute for checking a work out of the library. For exactly this reason, though, we suspect that this sort of arrangement is likely to be politically unacceptable.

A second-best alternative would require that the agent keep records of the applications and keys issued, but would subject the records to stringent privacy protections similar to those that now protect

---

[47] *See* A. Michael Froomkin, *It Came From Planet Clipper: The Battle Over Cryptographic Key "Escrow"*, 1996 U. CHI. LEGAL F. 15; Hal Abelson, et al., *The Risks of Key Recovery, Key Escrow, and Trusted Third Party Encryption* (1998), <http://www.cdt.org/crypto/risks98/>.

many library patron records. We think it likely that the copyright industries would demand the ability to match keys with identities so that the subsequent appearance of pirated materials could be linked to the applicants for access.[48] However, we would recommend that identifying information be released only pursuant to a court order, and only on a showing of *actual* piracy, as distinct from garden-variety infringement or arguable fair use. This places some evidentiary burden on the copyright holder, but we note that this mechanism nonetheless would give rights owners a substantial advantage that they do not enjoy for works distributed in traditional media. In addition, regulations governing the privacy practices of trusted third parties should prohibit sale or other transfer of key access information, and should require that access and usage records be destroyed after some period of time. We are cautiously optimistic that rigorous privacy protections could prevent the use of key access information to intimidate critics, parodists, and the like. Nonetheless, we label this arrangement "second-best" because even the most stringent system of privacy protections for fair users is likely to chill some lawful uses.

C. Mixed Fair Use Infrastructure

Each of the two possible mechanisms for preserving fair use in a digital rights management environment has advantages and drawbacks. Automatic fair use functionality does not require human intervention, but is unlikely to afford the full spectrum of fair uses allowed by law. The use of a trusted third party intermediary to mediate access, in contrast, potentially allows the full spectrum of uses but is less responsive to anonymity and spontaneity concerns. The optimal result, we suggest, is an infrastructure that combines the two.

The first layer of our proposed fair use infrastructure would involve the design of rights management technologies that incorporate automatic fair use defaults based on customary norms of personal noncommercial use. The legal rule for facilitating this part of the proposal would operate in a fashion similar to current provisions of the Copyright Act designed to encourage copyright registration and deposit, by conditioning copyright enforcement on implementation of the automatic fair use defaults.[49] To guard against a "race to the bottom" in fair use law, the law would clearly state that the level of copying permitted by the automatic defaults does not define the full extent of permitted fair use.

---

[48] Tying pirated materials to fair use applicants would require issuing unique keys to each applicant, or by means of "digital watermarks"; one or both of which appears to be within the realm of current technology.

[49] *See* 17 U.S.C. §§ 405(b), 411(a), 412; *see also infra* Part IV (discussing treaty compliance issues).

Those who desire greater fair use access, meanwhile, would turn to a trusted third party intermediary. Under the system, deposit of access keys into key escrow would be facilitated by conditioning anti-circumvention protection on such deposit. Users who failed to obtain access via the escrow agent would be subject to suit for circumventing technical measures; those users, however, still might escape liability by successful invocation of a constitutional defense to circumvention liability. Rights holders that opt not to deposit keys with the escrow agent would be unable to invoke legal protection against circumvention; for such unescrowed works, a "right to hack" would effectively substitute for access via the escrowed keys. As noted in Part II, the DMCA's ban on the manufacture and distribution of circumvention technologies also would need to be modified or amended to make this defense a realistic possibility. Finally, to preserve the relative anonymity of the key escrow system, the records of applicants and keys issued would need to be guarded by stringent legal protections along the lines described above.

The most likely and appropriate escrow agent will be a publicly funded institution, such as the Library of Congress; indeed, the Library's long experience with copyright matters and with deposit of copyrighted works makes it the ideal candidate to fill the escrow role. We see little prospect for development of private escrow agents, as has been the case in the trusted third party models for commercial PKI. Fair users are almost by definition poor candidates to fund an escrow institution. As we have indicated above, moreover, the point of fair use is to provide low cost or free access to content; assessing fair use fees to fund escrow agents would run counter to this purpose. Content owners, meanwhile, are unlikely to voluntarily pay for an institution that facilitates low cost or free access to their works.[50] Even were they to do so, however, a publicly funded institution probably would be the preferred choice because the public policies underlying fair use require some guarantee of institutional longevity. Finally, the tradition of strong privacy protection by libraries makes these institutions 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 administrative fee levied on copyright owners, or by some combination of the two.

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

[50] But see the data processing industry's efforts at "self regulation" in the face of threatened privacy legislation.

would go a long way toward approximating traditional fair use conditions. We turn now to consideration of whether the proposal is feasible as a matter of law and desirable as a matter of policy.

IV. TREATY CONSTRAINTS

A critical consideration in evaluating the feasibility of the system proposed here is whether legally induced automatic fair use defaults and legally induced escrow of rights management keys comport with the obligations imposed on the United States by international copyright treaties. Here, we consider the proposal's compatibility with the WIPO Copyright Treaty, the underlying Berne Convention for the Protection of Literary and Artistic Works, and the Agreement on Trade Related Aspects of Intellectual Property Rights (TRIPs). We conclude that the proposal passes muster under all of these agreements.

As an initial matter it might seem that our proposal would be most likely to run afoul of the provisions of the WIPO Copyright Treaty; after all, the passage of the current DMCA was purported to be necessary to bring United States copyright law into line with its obligations under that treaty. As Pamela Samuelson has explained, however, prior to the enactment of the DMCA, the doctrines of contributory infringement and vicarious liability already satisfied the treaty's requirement of "adequate legal protection and effective legal remedies" against circumvention of technological measures.[51] Even amended as we propose, the DMCA's anti-circumvention measures would go well beyond what the treaty requires. Moreover, the Agreed Statements accompanying the treaty include a declaration that signatory countries may continue to recognize existing limitations and exceptions to copyright, including fair use, as appropriate in the digital environment; and also may create new exceptions and limitations as appropriate.[52] This intepretative provision expressly contemplates the continued viability of fair use under the treaty. Our proposal simply would implement the contemplated fair use norm – and would do so in a way that largely preserves the more-than-adequate anti-circumvention protections that Congress created.

We turn next to consideration of the key escrow proposal in light of the older Berne Convention, which the WIPO treaty was intended to update. Under Article 5(2) of Berne, "[t]he enjoyment and the

---

[51] *See* WIPO Copyright Treaty, art. 11; Samuelson, *supra* note __, at 530-32.

[52] Agreed Statement Concerning the WIPO Copyright Treaty, Dec. 20, 1996, <http://www.wipo.org/eng/main.htm> (visited Aug. 17, 2000).

exercise of [copyright] shall not be subject to any formality."[53] It is unlikely that the key escrow system proposed here would run afoul of this requirement. The deposit requirement we propose here is not addressed to the work, nor to the copyright in the work, but only to the rights management system protecting a work. Deposit is not a condition of copyright protection for the underlying work, but is required only for the copyright holder to enjoy anti-circumvention protection. Absent a deposit, the copyright holder is still fully protected by copyright law against unauthorized copying in the event that the work's rights management system is circumvented. Copyright owners will enjoy all the rights required under Berne whether or not they choose to take advantage of the opportunity for anti-circumvention protection.

We believe that a rule conditioning copyright enforcement on the adoption of programmed fair use defaults also comports with the requirements of Berne, at least to the same extent as other provisions of United States copyright law. Prior to the United States' accession to the Berne Convention, United States copyright law was rife with technical formalities, the violation of which could forfeit the copyright in a work.[54] After accession, such formalities are no longer a prerequisite for obtaining or keeping a copyright; copyright subsists automatically upon the fixation of the work in a tangible medium of expression and cannot be forfeited by administrative oversight. Thus, United States law complies with the letter of Article 5(2). Nonetheless, the copyright in a work of United States origin cannot be enforced in court until the work has been registered.[55] Moreover, if a work is not registered promptly after creation, the copyright owner forfeits any future right to statutory damages or attorneys' fees.[56] Additionally, although notice is no longer a requirement for copyright protection, failure to place a copyright notice on a

---

[53] Berne Convention for the Protection of Literary and Artistic Works, art. 5(2) (1971).

[54] *See, e.g.*, 17 U.S.C. § 405 (1988) (requiring notice of copyright but allowing five years to cure omissions); Copyright Act of 1909, §§ 10, 19 *et seq*. (requiring notice of copyright). The United States joined the Berne Convention in 1989. *See* Berne Convention Implementation Act, Pub. L. 100-568, 102 Stat. 2853 (1988).

[55] *See* 17 U.S.C. § 411(a) (requiring registration of copyright as prerequisite for an infringement action for United States works).

[56] *See* 17 U.S.C. § 412 (prohibiting awards of statutory damages or attorneys' fees for infringement occurring after publication but before registration, unless registration is made within three months after first publication).

work may allow defendants to raise an "innocent infringer" defense in an enforcement action.[57] Our proposed rule is patterned after these provisions. We believe that our proposal is a legitimate and entirely defensible effort to balance two sets of obligations that must both be honored: the United States' obligations under Berne and the constitutional policies underlying fair use.

Finally, we must consider whether the proposal for programmed fair use defaults plus key escrow comports with the United States' obligations under TRIPs. TRIPs, like the Berne Convention, requires minimum standards of intellectual property protection and also makes provision for limited exceptions to such protection.[58] As in the case of Berne, TRIPs appears to contemplate the United States' conception of fair use as one of the allowable exceptions.[59] Moreover, TRIPs imposes no requirement of anti-circumvention protection at all. Thus, the treaty is at worst silent on the question, and much more arguably amenable to the policy and practices that the proposal would further.

Moreover, we believe that other language in the TRIPs agreement complements and even encourages the system we have outlined here. Article 40 specifically acknowledges that "some licensing practices or conditions pertaining to intellectual property rights . . . restrain competition" and "may have adverse effects on trade and may impede the transfer and dissemination of technology."[60] Article 40(2) authorizes member states to enact legislation regulating "licensing practices or conditions that may in particular cases constitute an abuse of intellectual property rights having an adverse effect on competition in the relevant market."[61] Specific examples of competitive restraints that states may individually address include "conditions preventing challenges to validity and coercive package licensing."[62]

---

[57] *See* 17 U.S.C. § 405(b) (exempting innocent infringers who prove reliance on lack of notice from infringement liability).

[58] With respect to copyrights, TRIPs largely incorporates the requirements of the Berne Convention. *See* General Agreement on Tariffs and Trade, Agreement on Trade-Related Aspects of Intellectual Property Rights, art. 9(1) (1994), Marrakesh Agreement Establishing the World Trade Organization, Annex 1C.

[59] *See id*. art. 17.

[60] *Id*. art. 40(1).

[61] *Id*. art. 40(2).

[62] *Id*.

In the context of digital rights management, we must consider as an initial matter whether this language may be properly applied to technical controls upon intellectual property. This language appears primarily directed toward particularized regulation of unfair competition, including anticompetitive practices that in the United States are considered matters for antitrust law. As we have noted above, by instantiating terms that might otherwise be conveyed by written licenses, technological controls will in many instances constitute the equivalent of such licenses, and thus also constitute a "licensing practice or condition" that is covered by the TRIPs language. Even if the controls are not themselves considered to be the equivalent of licenses, they will frequently be accompanied by written licenses, and so again would constitute a "licensing practice or condition."

We think that our proposal for programmed fair use defaults plus key escrow is a reasonable implementation of the language of the preamble and Article 40(2) of TRIPs. To take just one example, courts have recognized fair use as a legal vehicle to ensure access to copyrightable works for purposes of reverse engineering to create competing products or for technical interoperability. Although the DMCA includes a provision allowing circumvention of rights management systems for reverse engineering purposes, the provision is quite narrow and does not cover the range of reverse engineering activities that would be legitimate under current formulations of fair use access.[63] Additionally, software shrinkwrap licenses now routinely include provisions that purport to require surrender of a purchaser's fair use reverse engineering rights as a condition of access to the program. These technological and contractual restrictions surely constitute a condition "impeding transfer and dissemination of technology." The system proposed here would remedy this problem.

The proposed fair use infrastructure does not violate any treaty obligations concerning the protection of copyrighted works, and arguably advances other treaty goals. Thus, neither technology nor law stands as an obstacle to implementation of the proposed fair use infrastructure. We turn, finally, to consideration of whether other factors might do so.

---

[63] *See* 17 U.S.C. § 1201(f); Julie E. Cohen, *WIPO Treaty Implementation in the United States: Will Fair Use Survive?*, 21 EUR. INTELL. PROP. REV. 236, 239 (1999); Samuelson, *supra* note __.

V. COUNTERARGUMENTS (OR, THE RISKS OF SOCIAL ENGINEERING)

Here, we step back and consider whether our proposal for a mixed rights management infrastructure is wise. We have argued that legislative action can alter the direction of technological change. This may make things better – think, for example, of federal regulations mandating first seatbelts and later airbags in passenger cars – but it can also make them worse. For example, the congressionally mandated adoption of "wiretap ready" telephone switching equipment has led to weakened protection for many important attributes of private communications.[64] The DMCA itself is a sobering example of an ill-conceived legislative decision to favor one technological trajectory over others. Legislative changes also may trigger undesirable technological responses that Congress did not intend or foresee. Larry Lessig, for example, has persuasively argued that the development of anti-pornography filterware that permits targeted censorship is a technological development far worse than the cyber-zoning legislation it was designed to forestall.[65] Might our proposal have a similar effect? (Are our proposed changes more like airbags, or more like "censorware"?) Is our insistence on the possibility of productive congressional action naive? As Jessica Litman reminds us, copyright-related legislation has repeatedly proved itself especially vulnerable to capture by special interests.[66] Might a different sort of legal response to copyright management systems be better?

Our proposal for a mixed fair use infrastructure is inferior to traditional fair use rights in two respects. First, it would fail to permit the full degree of spontaneity enjoyed by fair users in nondigital media. Even a well-designed set of automatic defaults will not permit every use that a court might deem fair. And even a streamlined internet-based procedure for obtaining keys will inhibit spontaneity, and will

---

[64] Susan Freiwald, *Uncertain Privacy: Communication Attributes After the Digital Telephony Act*, 69 S. Cal. L. Rev. 949 (1996).

[65] Lawrence Lessig, *What Things Regulate Speech*, 38 JURIMETRICS J. 629 (1998).

[66] Jessica Litman, *Revising Copyright Law for the Information Age*, 75 OR. L. REV. 19 (1996); Jessica Litman, *The Exclusive Right to Read*, 13 CARDOZO ARTS & ENT. L.J. 29 (1994); Jessica Litman, *Copyright Legislation and Technological Change*, 68 OR. L. REV. 275 (1989).

impose transaction costs that users of nondigital media need not incur.[67] Realistically, too, there will be server outages and other technical difficulties that prevent fair users from obtaining keys.

Second and more important, the proposal (in its second-best incarnation) protects privacy, not anonymity. Traditional fair users have enjoyed both; there is no central (or distributed) database containing their names and contact information. We suspect that many who rely on fair use to produce and distribute their own information goods – academic works of critical commentary, software created through reverse engineering, and so on – do not desire anonymity in the long run. Yet anonymity is an indispensable facilitator for other types of criticism, and other types of exploration. And arguing that anonymity is the special province of "pirates" rather than legitimate fair users seems akin to arguing that wiretaps do not threaten innocents who have nothing to hide. In our view, both arguments are equally specious. Thus, we think that for our "second-best" system to be tenable, the privacy protections for fair users who access escrowed keys must be extraordinarily robust. Indeed, we wish to stress that this paper should not be construed as support for any version of our proposal that incorporates weaker privacy protection.

Adoption of the proposal also should not foreclose other measures to preserve anonymity. As we have noted, a key escrow system for fair use beyond that allowed by the programmed defaults would not preclude individuals who elect to hack copyright management systems from raising constitutional defenses to a lawsuit or prosecution under the DMCA's anti-circumvention provisions. In addition, it is worth repeating that anonymity and privacy are concerns not only of fair users, but also of users generally.[68] Fashioning anonymity and privacy protections for readers in the era of digital rights management is a subject beyond the scope of this paper. For example, though, Congress could – and, we would argue, should – direct that copyright management systems be designed, insofar as possible, to honor anonymous payment systems.

In sum, the proposal is a second-best solution designed to make the best of a bad situation. Rights management systems threaten to destroy fair use of digital materials, and to eliminate spontaneity and

---

[67] As one supporter of rights management has argued, however, users of nondigital works incur other sorts of transaction costs. *See* Tom W. Bell, *Fair Use vs. Fared Use: The Impact of Automated Rights Management on Copyright's Fair Use Doctrine*, 76 N.C. L. REV. 557 (1998).

[68] *See* Cohen, *A Right to Read Anonymously*, *supra* note __.

anonymity for would-be fair users and for readers generally. Our proposal accepts that these systems will be implemented, and strives to minimize their ill effects on socially valued uses. This raises the question whether we, too, are taking rights management systems as given, and thereby foreclosing a better solution to the problem of preserving fair use in the digital environment.

What might another solution look like? First, the Copyright Office might establish a set of exemptions to the DMCA's ban on circumvention of rights management technologies that preserves the traditional spectrum of fair uses.[69] In fact, we think this result unlikely. But even if the Copyright Office were to declare meaningful exemptions to the ban on circumvention, the separate statutory ban on the manufacture and distribution of circumvention technologies would render the exemptions meaningless, and would necessitate a court challenge to the statute itself.[70]

Next, following such a challenge, a court might declare the DMCA's anticircumvention provisions unconstitutional in their present form. Afterward, individuals seeking to make fair use of protected works would enjoy a right to hack the protective technologies without fear of civil suit or criminal prosecution. As a result, protection-defeating technologies would become more readily available, and simpler to use. Our proposal expressly provides for this result, of course, but it is likely that the availability of the programmed-default and key-escrow alternatives for fair use would decrease the incentives to mount such a challenge.

We note, first, that the DMCA's early airings in the federal district courts do not inspire faith in these predictions.[71] Assuming, however, that the courts of appeal show more backbone, we think that under a fair use regime defined by constitutional litigation, individuals seeking access to encrypted or otherwise protected digital works still will enjoy materially less fair use, and less spontaneity and anonymity in fair use, than they do now. Although a court might (and in our view, should) declare the

---

[69] *See* U.S. Copyright Office, *Exemption to Prohibition on Circumvention of Copyright Protection Systems for Access Control Technologies*, 64 FED. REG. 66,139 (Nov. 24, 1999); U.S. Copyright Office, *Rulemaking on Exemptions from Prohibition on Circumvention of Technological Measures that Control Access to Copyrighted Works*, <http://www.loc.gov/copyright/1201/anticirc.html> (visited Aug. 16, 2000).

[70] *See* 17 U.S.C. § 1201(a)(1)(E) (stating that exemptions to ban on act of circumvention shall not serve as defenses to other provisions); *id*. § 1201(a)(2), (b) (prohibiting the manufacture, distribution, or importation of circumvention technologies).

[71] *See* Microsystems Software, Inc. v. Scandinavia Online, 98 F. Supp. 2d 74 (D. Mass. 2000); Universal City Studios, Inc. v. Reimerdes, 82 F. Supp. 2d 211 (S.D.N.Y. 2000).

anticircumvention provisions facially invalid, a far likelier result is that decisions as to constitutionality would be made on a piecemeal, as-applied basis. Thus, the threat of prosecution or suit under the DMCA will continue to chill many lawful fair use activities. Even facial invalidation of anticircumvention legislation, moreover, will not prevent private publishers from implementing rights management systems. Congress might do so, of course, but we think it inconceivable that Congress would pass such a law. And even the most user-friendly circumvention technologies will require some threshold level of technological competence.

There remains, finally, the question whether successful court challenges to the DMCA's anti-circumvention provisions might create incentives for content owners to design their systems more flexibly, to accommodate a degree of spontaneous, anonymous fair use. For example, the prospect of costly litigation of repeated constitutional challenges might provide incentive to incorporate into works steganography (watermarking technology) that could the proliferation of a certain digital work to be traced back to particular distribution points or copies, or even to particular user.[72] Conceivably, this might move copyright holders toward steganography alone as a method of deterring digital piracy. This state of affairs would tend to support spontaneous fair use of digital materials much better than would a proliferation of "lock-out" systems and fair use preauthorization requirements.

We think, though, that a system of programmed fair use minima plus key escrow requirements probably would create even stronger incentives for more flexible design. Most obviously, our proposal would require a minimum degree of system flexibility as a condition of state-backed copyright enforcement. Although private ordering has become increasingly central to copyright enforcement strategies, the copyright industries continue to view a degree of state-backed enforcement as essential.[73] In addition, we cannot unqualifiedly endorse steganography as the magic solution to the problem of fair use under rights management. A system for steganography-based rights management that attempted to register unique copies to identified users would destroy anonymity for fair users, and indeed for all

---

[72] *See* NII WHITE PAPER, *supra* note __, at 188-89; Kenneth W. Dam, *Self-Help in the Digital Jungle*, 28 J. LEGAL STUD. 393 (1999); Rosemarie F. Jones, *Wet Footprints? Digital Watermarks: A Trail to the Copyright Infringer on the Internet*, 26 PEPPERDINE L. REV. 559, 569 (1999).

[73] Imposing the "carrots" of mandatory fair use minima and key escrow might of course diminish the preference for state enforcement. However, our faith in the ingenuity of hackers is such that we do not think a system of pure private ordering would be in the copyright industries' best interests.

readers. Although we think that steganography offers certain advantages over other forms of rights management – and that a steganography-based system need not be designed to compromise anonymity (or privacy) – we think that the legitimacy of such a system would depend on the specific details of its implementation.

Returning, finally, to the example of filterware, it seems highly likely that the market would have developed filterware whether Congress had passed legislation zoning internet pornography or not. We cannot say the same for our proposal, and we think this is one of its strengths. Where copyright management systems are concerned, the market drives inexorably toward ever-less-flexible controls – or, rather, for controls that are flexibly responsive to the business plans of rights-holders, not the desires and habitual practices of fair users. A move toward greater flexibility will require some other impetus. We think that our proposal could provide this impetus. At the least, we hope that it will encourage greater discussion of the possibilities.