

## **Legal and Technical Standards in Digital Rights Management Technology\***

Dan L. Burk<sup>†</sup>

### **I. Introduction**

Copyright and similar exclusive rights regimes have long been mainstays of innovation policy, purporting to provide the incentive necessary to generate creative and innovative products for the benefit of the public. The received economic wisdom holds that a period of legal exclusivity allows the developer of a new creation to recoup the investment made in development, either by selling the product at higher than marginal cost, or by licensing the work to others who will sell it at higher than marginal cost.<sup>1</sup> The supranormal profits generated by excluding the creation or its close substitutes from the marketplace provide the incentive for the initial investment in what we term “intellectual property.”

To be sure, the promise of a return on investment is important for the development of all kinds of goods, not merely those we term intellectual property. But many products of human endeavor require little or no developmental encouragement by way of legal exclusion, as these goods carry naturally in their form or design the attributes of exclusivity in their form or design. While tangible goods generally benefit from some legal protection against theft, there is already a considerable cost to

---

\* Copyright 2004 by Dan L. Burk.

<sup>†</sup> Oppenheimer, Wolff & Donnelly Professor of Law, University of Minnesota.

<sup>1</sup> See See William M. Landes & Richard E. Posner, *An Economic Analysis of Copyright Law*, 18 J. LEGAL STUD. 325 (1985).

misappropriation such goods, and the cost is often substantial enough both to deter pilferage of these products, and ensure a return on the investment needed to create them. Absent a radical departure from the usual laws of physics, it is difficult to walk away with a building<sup>2</sup>, or to feed a multitude with five loaves and a two fish.<sup>3</sup> Height, depth, breadth, weight, mass, and entropy endow tangible goods with a ready-made scarcity.

However, where the primary value of a good lies in its creative or innovative character, rather than in its physical qualities, the resistance of tangible form to tangible appropriation offers little natural deterrence to appropriation of its more ephemeral qualities. Individual instantiations of intellectual property are certainly embodied in particular physical forms – on paper, on canvas, on magnetic or optical media – that can be guarded from a physical theft.<sup>4</sup> But once the physical object is made accessible, by publication, sale, or otherwise, the ideas, information, or artistic content embodied become exposed to copying or imitation.

The potential for such copying or imitation of intellectual property is generally a function of technological progress. In particular, recent advances in computer and networking have greatly enabled the appropriation of ephemeral products. Digitization eliminates much of the physical character of creative works, embodying creativity as ethereal bits rather than material atoms. As digital technology proliferates and becomes

---

<sup>2</sup> See Lawrence Lessig, *Constitution and Code*, 27 CUMB L. REV. 1 (1997)

<sup>3</sup> See Matt. 16-21; Matt. 15:32-38; cf. Exodus 16:4. One of the common themes of mythologies around the world is that, terrestrial scarcity notwithstanding, the gods miraculously provide private goods as if they were public goods. See Hugh Nibley, *Work We Must, But the Lunch is Free*, 202, 217 in *APPROACHING ZION: THE COLLECTED WORKS OF HUGH NIBLEY, VOL. 9* (Don E. Norton, ed., 1989).

<sup>4</sup> See I. Trotter Hardy, *Not So Different: Tangible, Intangible, Digital, and Analog Works and Their Comparison for Copyright Purposes*, 26 DAYTON L. REV. 211 (2001). In copyright, the distinction between creative character and particular physical instantiations is maintained by the legal definition of “copy” and “work.” See 17 U.S.C. § 101. Failure to maintain the distinction between the copy and the work can lead to serious analytical error regarding the treatment of the work’s creative value. See, e.g., Hardy, *supra*.

increasingly interconnected, regimes of legal exclusion become increasingly difficult to police and enforce.<sup>5</sup> Reproduction and distribution of materially embedded works required the costly technology to manipulate and transport tangible products, and so limited the capability for unauthorized appropriation to a relative few, highly-capitalized actors; but the technology to accomplish digitized reproduction and distribution is now available at low cost, transforming individuals of relatively modest means into potential infringers.

While the proliferation of digital technology raises the cost of policing and enforcing legal exclusion, the same technology may also offer the producers of intangible goods an alternative method of exclusion. Because digital technology is capable of virtually modeling structural reality<sup>6</sup>, it can be programmed to mimic the characteristics of tangible property. Producers of intellectual property may therefore resort to a form of self-help by re-embedding intangible goods in digital rights management systems, or DRM, that simulate the natural appropriability resistance of physical goods.<sup>7</sup> Such technological controls prohibit or constrain the copying and distribution that digital formats invite. By essentially transforming public goods back into private goods, owners of intellectual property may introduce into the design of digital media the more congenial constraints of more traditional media. Indeed, the constraints imposed by DRM may in some cases be designed to exceed those of traditional media.

But in order to reproduce the natural constraints of tangible form, DRM must user interaction with the same predictability as physical matter. The goal of deploying reliable

---

<sup>5</sup> See COMPUTER SCI. & TELECOMM. BD., NAT'L RESEARCH COUNCIL, THE DIGITAL DILEMMA: INTELLECTUAL PROPERTY IN THE INFORMATION AGE (2000).

and deterministic constraints on user behavior simultaneously drives the character of this self-help technology in relation to both legal and technical standards.<sup>8</sup> This definition of DRM occurs simultaneously in two different contexts with similar labels. The terminology of “standards” has been employed differently, and to some extent contrarily, in legal and technical parlance.<sup>9</sup> In legal discourse, “standards” nomenclature has referred to flexible and fact-specific legal imperatives, used for *ex post* decisional determinations. In technological discourse, “standards” nomenclature has referred to uniform technical specifications. Yet, as I shall show in the following pages, these differing terminologies intersect and converge in the structure of DRM: as the goal of determinism confines the discretion and flexibility governing use of technologically protected materials, it also dictates uniformity and exclusivity in technological design.

In examining the relationship between these characteristics, I first take up the problem of DRM as a substitute for legal standards, describing the constraints imposed by adopting technological rather than legal protections. I then consider the influence of DRM on technological standards, including both the advantages and disadvantages of convergence on a preferred rights management technology. I discuss the impact of layering legal protection, in the form of anti-circumvention statutes, over such technical standards, with particular attention to the effects of such legal protections on competitive behavior. I turn then to a discussion of several recent cases that demonstrate these

---

<sup>6</sup> See Phil Agre, *Internet Research: For and Against*, in I Internet Research Annual: Selected Papers From The Association of Internet Researchers Conferences 2000-2002, at 25, 27 (Mia Consalvo et al., eds., 2004).

<sup>7</sup> See generally, Mark Stefik, *Trusted Systems*, SCI. AM. March, 1997 at 78.

<sup>8</sup> J. S. Erickson & Deirdre K. Mulligan, *The Technical and Legal Dangers of Code-Based Fair Use Enforcement*, 92 PROC. IEEE 985 (2004).

<sup>9</sup> Daniel Benoliel has recently made a similar point along these lines. See Daniel Benoliel, *Technological Standards, Inc. Rethinking Cyberspace Regulatory Epistemology*, 92 CAL. L. REV. 1069, 1091 (2004) (proposing a new nomenclature for technical standards due to their centralized regulatory nature).

effects, but that also demonstrate emerging judicial initiatives to ameliorate the potential for anti-competitive outcomes. I conclude by considering the prospects for these judicial initiatives, and the need for further reforms.

## **II. Regulatory Design**

The design of technological artifacts may be shaped by a variety of factors: the cost of production, the availability of materials, the expectation of purchasers, even the current whims of fashion. Each of these social and economic factors affects the characteristics of the product, and, ultimately, the way in which the artifact may be used. Indeed, products will typically be designed with certain uses in mind, and so imbued with characteristics that allow some uses, and disallow other uses. In some cases, behavior is inadvertently channeled via routine technological design decisions regarding the size, shape, material, or placement of everyday artifacts. But frequently size, shape, material, or placement of artifacts is calculated to produce a particular result.

Thus, DRM constitutes an exceptionally complex and sophisticated attempt to delimit the behavior of consumers, but is hardly the first such attempt, nor the most prevalent. The intentional design of technologies to constrain or prompt certain behaviors is relatively common. For example, Bruno Latour illustrates his discussion of such constraints via the example of speed bumps along a roadway. These intentional bumps in the road are safely negotiated at lower speeds, but cause uncomfortable jolts, as well as potential damage to automobile suspension systems, if the mild obstructions are negotiated at higher speeds. Latour dubs these structures “sleeping policemen,” as they

serve to keep traffic speeds down, accomplishing much the same result as posting actual traffic officers along the route.<sup>10</sup>

As the example of speed bumps suggests, the interaction between the design of human artifacts and the users of those artifacts defines certain types of behavior accompanying the artifact. Scholars studying the social effects of technology have long observed that such “social shaping” is routinely accomplished through design that recruits the end user into a particular social role.<sup>11</sup> As in a stage play or film, roles follow a particular instruction set, or script. But in the case of artifactual design, the script is built into the shape or characteristics of the artifact – user responses to the artifact are channeled into certain pre-defined roles. The shape, placement, and physical qualities of speed bumps compose a behavioral script prompting human drivers to slow down. In essence, the design of the speed bump is inscribed with the instruction “Slow Down.”

Such technological regulation or “scripting” is relatively easy to see in human artifacts, once one begins to look for it. “Child-proof” bottle cap configurations deter consumption of pharmaceuticals by children lacking the manual strength or dexterity to open the bottle. Pillars or other architectural barriers afford passages too narrow to accommodate the width of shopping carts, deterring removal and ultimate loss of shopping carts from the immediate premises of grocery stores. Turnstiles ratchet in one direction only, channeling subway riders or sports fan into a particular space via a particular route, and preventing exit through the same portal. One-way retractable

---

<sup>10</sup> Bruno Latour, *Where are the Missing Masses? The Sociology of a Few Mundane Artifacts* in *SHAPING TECHNOLOGY/BUILDING SOCIETY: STUDIES IN SOCIOTECHNICAL CHANGE* 225, 244 (Weibe E. Bijker & John Law, eds., 1992).

<sup>11</sup> See, e.g., Stephen R. Barley, *The Alignment of Technology and Structure Through Roles and Networks*, 35 *ADMIN. SCI. Q.* 61 (1990); Hugh MacKay et. al, *Reconfiguring the User: Using Rapid Application Development*, 30 *SOC. STUD. SCI.* 737 (2000); Steve Woolgar, *Configuring the User: The Case of Usability*

roadway spikes allow vehicles to proceed in one direction, as backing the vehicle up would risk “severe tire damage.”

In digital media, a similar physical design “script” might be illustrated by the recent production of DVDs that, much like the anonymous directive audio tapes in the old *Mission: Impossible* television show, self-destruct after use. The DVDs are formed of a substance that degrades after the packaging is opened, limiting the life of the product after purchase.<sup>12</sup> The discs are composed of a polymer that begins to darken when exposed to air; when the reaction reaches a certain degree of opacity, the data on the disc can no longer be read by the laser in a playback machine. The polymer can be formulated so that the darkening process takes twenty-four, forty-eight, or some other specified number of hours, so that the consumer essentially pays for a set period of access to the content. The process can reportedly be slowed by refrigeration, but eventual illegibility is an irreversible characteristic of the product's physical structure.

The design of such DVDs is significant in part because it allows the producer to price discriminate among purchasers with different preferences.<sup>13</sup> Purchasers who wish to view a movie once or twice can purchase for a low price a DVD that will be viable for 24 hours. Purchasers who may wish to view a movie multiple times can for a higher price purchase a DVD with a longer lifespan. Purchasers who may wish a permanent copy of the movie, to be held in the purchaser's video library and viewed multiple times presumably attribute the greatest value to the movie and can be charged a relatively high price for a copy that does not self-destruct. The characteristics of the physical disc

---

*Trials* in A SOCIOLOGY OF MONSTERS: ESSAYS ON POWER, TECHNOLOGY, AND DOMINATION 57 (John Law, ed., 1991).

<sup>12</sup> Eric A. Taub, *DVDs Meant for Buying but Not for Keeping*, N.Y. TIMES, July 21, 2003, at C1.

carrying the movie determines the behavior of the purchaser toward the disc, and so the price that can be charged for the disc.

The adoption of such design-based behavioral regulation may sometimes be mandated by the state, or sometimes spontaneously adopted by private manufacturers, or a combination of both, depending upon the natural and desired incentive structure for adoption. Regulatory designs may be desirable where the cost of monitoring and enforcing the desired behavior via human agency is too high – the cost of situating actual policemen along every roadway in order to enforce speed limits would be prohibitive; speed bumps may prompt the desired speed limit compliance at a lower cost. In the case of DVDs, monitoring and policing the number of home viewings of a standard DVD, in order to charge according to consumer usage would be invasive and costly; offering time-limited DVDs allows consumer to self-select high or low value versions at the point of purchase.

The relative cost of such self-enforcing mechanisms is equally important when determining whether to employ regulatory designs or other behavioral mechanisms to reach a desired result. In particular, regulatory design can in some instances serve as a substitute for legal regulation. Thus, Latour's "sleeping policemen" may act as a speed limiting device even in the absence of a formal statute or ordinance regulating vehicular speed. Latour similarly describes how automobile seatbelts with ignition interlocks, which require the seatbelt to be buckled before the ignition will start, embody type of "script" requiring a driver to take the particular action of fastening the seatbelt before

---

<sup>13</sup> See Michael Meurer, *Price Discrimination, Personal Use and Piracy: Copyright Protection of Digital Works*, 45 Buffalo L. Rev. 845 (1997).

driving.<sup>14</sup> This requirement might otherwise be enforced by a statute or ordinance requiring the use of seatbelts. Similarly, a locked door effectively embodies a “script” or rule against unauthorized entry, whether or not a formal law forbids such unauthorized entry.

Dozens of such examples could be cited, and the interaction between regulatory design and regulatory enactments is complex. Frequently both are used as complements or reinforcements for one another in order to produce the desired behavioral outcomes. This is particularly the case where regulatory designs would provide the most efficient means for prompting a particular behavior, but due to externalities, the incentives to adopt such designs are lacking or improperly distributed. Consider, for example, the in which the state wishes to enforce safety standards by requiring all automobile drivers to use seat belts.<sup>15</sup> The most direct method to produce the desired behavior is to pass laws penalizing the failure to use such harnesses, but this incurs law enforcement costs to detect and punish driving without buckling up. An alternative method to produce the desired behavior, suggested by Latour, is to fit automobiles with seatbelt ignition interlocks; but this must be done by the manufacturer, at a cost that will likely be passed on to consumers, resulting in higher prices for purchases and fewer sales for manufacturers. Neither may be willing to incur such costs in return for societal savings in safety that seems to each remote.

But the state may implement the technological alternative through a variety of regulatory mechanisms, from a variety of sources. Most directly, the state might simply

---

<sup>14</sup> See Latour, *supra* note \_\_, at 225-26; see also Madeleine Akrich, *The De-Description of Technical Objects* in SHAPING TECHNOLOGY/BUILDING SOCIETY: STUDIES IN SOCIOTECHNICAL CHANGE 205 (Weibe E. Bijker & John Law eds 1992).

<sup>15</sup> Latour, *supra* note \_\_\_\_.

require automobile manufacturers to install seatbelt interlocks on all cars produced.<sup>16</sup>

Alternatively, courts, or legislatures acting through courts, could impose liability for deaths or injuries on manufacturers who fail to install seatbelt interlocks, creating an incentive to include the feature in cars. Similar liability could be imposed on car drivers or owners, creating a consumer demand for manufacturers to install the devices.

Ancillary social actors, such as insurers, may also be mobilized to ensure installation of the technological feature. For example, if liability is imposed on drivers who fail to adopt the technology, insurance payments for such drivers will likely increase. Insurers will presumably decrease premiums for drivers who lessen their liability by adopting the technology, partially subsidizing the cost of adoption. These alternatives may be superior to a direct design mandate, potentially invoking market forces to develop better versions of the technology at cheaper prices, rather than requiring adoption of a particular technological configuration by state fiat.

While the example of seatbelts or speed bumps largely implicate technological design as a substitute or complement for the public goods mediated by tort and criminal law, regulatory designs can also substitute for contract where private transactions are concerned. For example, it is possible to consider the design of a limited-use DVD, facilitating producer price discrimination, as a substitute for contractual provisions designed to accomplish a similar end. Such contractual provisions may be used to limit product uses in ways that intellectual property law does not. Copyright law affords the owners of digital content recourse against many unauthorized uses of their material, but copyright is subject to a host of uses that require no authorization from the copyright

---

<sup>16</sup> See J. MASHAW & D. HARFST, *THE STRUGGLE FOR AUTO SAFETY* (1990).

holder.<sup>17</sup> Prominent among these is the ability of a purchaser to dispose of a copy by resale or other means under copyright's "first sale" doctrine. Under this doctrine, ownership of the incorporeal work and ownership of the tangible embodiment are effectively bifurcated. Thus, a consumer may purchase a book or painting or DVD and may typically dispose of the physical object however she pleases – by reselling it, giving it away to a friend, tossing it into the trash bin, setting it on fire. What the owner of the physical object typically may *not* do is to dispose of it in one of a small number of restricted manners that implicate the embodied work – using the object as a template for making additional copies, for example.

A scheme of price discrimination is nearly impossible to maintain under such conditions, as the supplier of the intangible work is unable to prevent buyer arbitrage.<sup>18</sup> Low-valuing purchasers might obtain DVDs and resell them to at higher prices to high-valuing purchasers, bypassing the DVD producer, and pocketing the surplus. Owners of digital content have long wished to escape the first sale doctrine and similarly inconvenient consumer privileges afforded by copyright law. They have attempted to do so through the fiction of the "shrink-wrap" or "click-wrap" license, which purports to restrict a purchaser's use of the accompanying product.<sup>19</sup> The license takes its name from the legal fiction that the purchaser demonstrates agreement to the license terms by breaking the "shrinkwrap" cellophane on the product package, or, more recently assent

---

<sup>17</sup> See, e.g., 17 U.S.C. §§ 107-112 (detailing numerous and varied exceptions to the exclusive rights of the copyright holder, such as the right to perform non-dramatic musical works at agricultural fairs, or in the classroom).

<sup>18</sup> See Meurer, *supra* note \_\_\_\_.

<sup>19</sup> See David W. Maher, *The Shrink-Wrap License: Old Problems in a New Wrapper*, 34 J. COPYRIGHT SOC'Y 292 (1987); Deborah Kemp, *Mass Marketed Software: The Legality of the Form License Agreement*, 48 LA. L. REV. 87 (1987).

using the computer mouse cursor to click on a graphic labeled "I agree."<sup>20</sup> Because is styled as a license, rather than a sale, it negates the privileges afforded by first sale.

Such licenses might appear to provide a solution to the arbitrage problem faced by the producer of a copyrighted work, such as a movie contained in a DVD. A restriction on resale might be included as part of the license accompanying the work. However, the road to legal acceptance for such agreements has been long and tortuous.<sup>21</sup> Courts in the United States have in many cases been reluctant to enforce such agreements because in the classic shrinkwrap format, the purchaser may have no opportunity to review the license prior to opening the package.<sup>22</sup> In some circumstances, such licenses may be limited by contract doctrines of unconscionability, or preempted by federal policy governing the rights the contract seeks to allocate.<sup>23</sup> Some commentators have suggested that overreaching attempts to limit consumer exemptions and privileges granted under the statute could run afoul of federal copyright policy.<sup>24</sup> And even if such licenses become more frequently enforceable, it remains extremely difficult for copyright holders to police such agreements.

Consequently, regulatory design may be an attractive lower-cost alternative to policing and enforcing such legally troublesome agreements. But these lowered enforcement costs must be balanced against other, possibly significant costs entailed in

---

<sup>20</sup> Mark Lemley, *Shrinkwraps in Cyberspace*, 35 JURIMETRICS J. 311 (1995).

<sup>21</sup> See Robert A. Hillman & Jeffrey J. Rachlinsky, *Standard-Form Contracting in the Electronic Age*, 77 NYU L. REV. 429 (2002).

<sup>22</sup> See Mark Lemley, *Beyond Preemption: The Law and Policy of Intellectual Property Licensing*, 87 CAL. L. REV. 111 (1999); Mark Lemley, *Intellectual Property and Shrinkwrap Licenses*, 68 S. CAL. L. REV. 1239 (1995).

<sup>23</sup> See Niva Elkin Koren, *A Public-Regarding Approach to Contracting Over Copyrights* in EXPANDING THE BOUNDARIES OF INTELLECTUAL PROPERTY: INNOVATION POLICY FOR THE KNOWLEDGE SOCIETY 191 (Rochelle Cooper Dreyfuss, Diane Leenheer Zimmerman, & Harry First, eds., 2001).

<sup>24</sup> See David Nimmer, Elliot Brown, & Gary N. Frischling, *The Metamorphosis of Contract into Expand*, 87 CAL. L. REV. 17, 67 (1999).

adopting the design option. All regulatory design involves such costs – not simply the cost of the creating structure itself, but the costs implicit in the behavior deterred. Latour's "sleeping policemen" exact a price whenever excessive speed would be justified, as in an emergency, when police or rescue vehicles might be required to use the speed impaired roadway. "Child-proof" bottle caps may impair the fingers of the elderly; barriers intended to deter the theft of shopping carts may impede the access of shoppers in wheelchairs, or of shoppers employing strollers for children; turnstiles may create bottlenecks during rush hour or at times when a large crowd needs to move in the opposite direction – to exit the station or arena, for example.

These costs arise out of the inability of the design structure to accommodate unforeseen or unacknowledged contingencies. Unlike policemen, speed bumps lack the capacity to recognize and permit socially beneficial speeding. Child-proof vial caps lack the capacity to recognize and permit access to an individual who shares with children a lack of manual strength, but differs from children in maturity and discernment. Redesign that removes human agency also removes human discrimination, leaving potentially costly situations outside the access parameters of the design. If the costly contingent situations occur infrequently, the design structure may still net benefit. But if the contingent situations occur more frequently than expected, or are of a serious nature, regulatory design can become costly, although perhaps not to the same set of actors to whom the savings accrue – policemen rather than ambulances; the elderly rather than the very young.

This observation holds equally true where regulatory design is targeted to facilitate a private goal such as price discrimination. Price discrimination itself entails

costs, and may not always be beneficial from the standpoint of wealth transfer.<sup>25</sup> More importantly, the standard optimistic model of price discrimination assumes that the purchaser and the supplier of the good know and internalize the proper social value of the goods being exchanged, and factor that into the price. But some costs and some benefits may be unforeseen, unknowable, external to the parties, or simply too diffuse for them to contemplate. For example, past instances of the irretrievable cultural loss of important motion pictures due to unforeseen deterioration of available copies might give us pause when contemplating a future where many or most of the DVD copies of a motion picture are subject to *intentional* deterioration. The social and cultural importance of preserving a cultural work, and the survival value of having multiple intact copies of a motion picture in circulation, are not likely to be part of the pricing calculus for buyers or sellers in deciding whether to issue self-destructing DVDs. Similarly, there may well be important but unforeseen social value in having intact and unencumbered copies of motion pictures in the possession of purchasers – unconsidered entertainment value to another member of the household, unintentional inspirational value to a future director or producer, serendipitous educational value to a child who finds the disc upon a shelf. None of these positive externalities is likely to be taken into account in issuing or purchasing a self-destructing DVD, either.

---

<sup>25</sup> See Meurer, *supra* note \_\_\_\_; Julie E. Cohen, *Copyright and the Perfect Curve*, 53 VAND. L. REV. 1799, 1801 (2000).

### III. Embedded Rules

The physical character of self-destructing DVD effectively replaces a licensing provision directed to first sale, accomplishing the same end as a shrink-wrapped prohibition on resale, or limit on use. But the composition of such structures provides a relatively simple design script, replacing the behavior expected under a relatively simple contract. To induce more complex behaviors, of the sort expected under more complex contracts, would require product designs capable of incorporating more complex scripts. Computer software, for example, comprises a technological artifact that can be programmed or scripted to “behave,” that is, to perform complex functions specified by a programmer.<sup>26</sup> These complex functions are indeed “scripted,” arising from the grammatical quality of computer technologies that allows for explicit inscription of discourse within their design.<sup>27</sup> The physical construction of the door enforces a particular prohibition, just as the electro-mechanical “script” of the ignition interlock enforces its particular prohibition, but these artifacts are not programmable in the sense that software may be programmed with a wide range of attributes. To a far greater extent than speed bumps or seat belts, digital technologies carry the capacity to embody highly sophisticated behavioral inscriptions, that can accompany copies of a creative work as they are distributed, controlling uses of the work.<sup>28</sup> Consequently, because technological can be scripted to accommodate a variety of user behaviors, technological controls can be

---

<sup>26</sup> See Pamela Samuelson et al., *A Manifesto Concerning the Legal Protection of Computer Programs*, 94 *CEV. L. REV.* 2308 (1994) (describing software as a text that “behaves”).

<sup>27</sup> See Agre, *supra* note \_\_\_\_.

<sup>28</sup> See generally *THE DIGITAL DILEMMA* *supra* note \_\_ at 153-76; Mark Stefik, *Shifting the Possible: How Digital Property Rights Challenge Us to Rethink Digital Publishing*, 12 *BERKELEY TECH. L.J.* 138 (1997).

scripted to incorporate restrictions that might otherwise be the subject matter of a written license.

To this end, copyright owners have begun deploying sophisticated software “lock-out” systems that prevent access to digitized content except on the terms dictated by the owner.<sup>29</sup> These devices may take a variety of forms as hardware or software, or some combination of the two.<sup>30</sup> Such content management software, sometimes called “digital rights management” or “DRM” systems, may govern a wide range of user behaviors, such as the number of times a work may be accessed, or the duration of access, the ability to reproduce or transmit the work, or the payment schedule for additional access.<sup>31</sup>

Technological control systems may be used to prevent initial access to digital content without the permission of the content owner, for example, by provision of a password. Such access might be occasioned upon terms of payment or terms of usage for the protected content. The technology may also be designed to control behaviors that occur after access; for example, the DRM system might be programmed to permit only one playback of a work, or allow only one copy of a work to be printed. Technological control systems may tie access or use of the work to a certain machine, or when attached to a network or other signaling device, monitor the degree and type of use of the work, perhaps to meter payment by the minute, by the bit, or by some other unit of usage. They may allow different levels of use depending on the level of payment made. Contingent or alternative terms might be programmed into the system, allowing a single access for a

---

<sup>29</sup> See Julie E. Cohen, *Some Reflections on Copyright Management Systems and Laws Designed to Protect Them*, 12 BERKELEY TECH. L.J. 161 (1997); Kenneth W. Dam, *Self-Help in the Digital Jungle*, 28 J. LEGAL STUD. 393 (1999).

certain fee, or unlimited access for a higher fee. Access might even be revoked automatically, or by remote command, if payments are not made in a timely fashion.<sup>32</sup>

In any of these applications, the technological constraints programmed into the system provide a self-enforcing substitute for legal constraints.<sup>33</sup> For example, rather than agreeing in a written license that as a condition of access, the user will make only one copy of the content, the technological controls may be built to allow only one copy to be made.<sup>34</sup> Rather than agreeing in a written license that as a condition of access, the user will pay a fixed price for a copy of the content, the technological controls may be built to require a credit card number upon access, which account will via an Internet connection be charged an incremental price when a copy is made.<sup>35</sup> Technological protection may also be combined with legal mechanisms; for example, access to technologically controlled content may be provisioned on agreement to a clickwrap-type license that purports to restrict the permissible uses of the work.<sup>36</sup> Indeed, where technological controls are used in combination with “clickwrap” licensing the terms may be enforced by the control system itself.<sup>37</sup>

---

<sup>30</sup> See Eric Schlachter, *The Intellectual Property Renaissance in Cyberspace: Why Copyright Law Could be Unimportant on the Internet*, 12 BERKELEY TECH. L.J. 15, 38-45.

<sup>31</sup> See Mark Stefik, *supra* note \_\_.

<sup>32</sup> See Julie E. Cohen, *Copyright and the Jurisprudence of Self-Help*, 13 BERKELEY TECH. L.J. 1089 (1998).

<sup>33</sup> See Margaret Jane Radin, *Online Standardization and the Integration of Text and Machine*, 70 FORDHAM L. REV. 1125, 1138 (2002).

<sup>34</sup> See Tom W. Bell, *Fair Use v. Fared Use: The Impact of Automated Rights Management in Copyright's Fair Use Doctrine*, 76 N.C. L. REV. 557 (1998).

<sup>35</sup> See Charles Clark, *The Answer to the Machine is the Machine* in THE FUTURE OF COPYRIGHT IN A DIGITAL ENVIRONMENT 149 (P. Bernt Hugenholtz, ed. 1996).

<sup>36</sup> See Michael J. Madison, *Legal-Ware: Contract and Copyright in the Digital Age*, 67 FORDHAM L. REV. 1025 (1998).

<sup>37</sup> See Bell, *supra* note \_\_; Dean S. Marks & Bruce H. Turnbull, *Technical Protection Measures: The Intersection of Technology, Law, and Commercial Licenses*, 22 EUR. INTELL. PROP. REP. 198 (2000)

The implications of this development are striking. As both Larry Lessig<sup>38</sup> and Joel Reidenberg<sup>39</sup> have pointed out, technical standards are within the control of the designer, and so confer upon the designer the power to govern behavior with regard to that system.<sup>40</sup> Once constraints on behavior are built into the technical standards governing a technology, the technical standards effectively become a new method for governing use of that technology – in essence, the technical standards, or “code,” become a type of law. Such technical rule sets may supplement or even supplant the legal rule sets designed to govern the same behavior. For example, as described above, the copyright owner may decide that the technological controls will not permit any copying of the controlled content, whether or not the copying would be permissible under a statutory user exemption, such as fair use. Thus, by implementing technical constraints on access to and use of digital information, a copyright owner can effectively supersede the rules of intellectual property law.<sup>41</sup>

But even were the deployment of DRM intended to perfectly mirror the parameters of copyright law, technological controls and legal controls are not perfect substitutes for one another. The two forms of constraint differ in certain aspects, notably in the degree of discretion afforded to the user. Where legal regulation constitutes the barrier to use of content, users may breach it at their discretion, avoiding penalties until they are apprehended, if they are apprehended, and legal process is complete. But when

---

<sup>38</sup> LAWRENCE LESSIG, *CODE AND OTHER LAWS OF CYBERSPACE* (1999).

<sup>39</sup> Joel Reidenberg, *Lex Informatica: The Formulation of Information Policy Rules Through Technology*, 76 TEXAS L. REV. 553 (1998).

<sup>40</sup> See also Daniel A. Farber, *The Dead Hand of the Architect*, 19 HARV. J. L. & PUB. POL'Y 245 (1996) (observing how architectural design dictates academic social interaction); Neal Kumar Katyal, *Architecture as Crime Control*, 111 YALE L.J. 1039 (2002) (discussing building and neighborhood design to channel behavior).

<sup>41</sup> See Glynn Lunney, *The Death of Copyright: Digital Technology, Private Copying, and the Digital Millennium Copyright Act*, 87 VA. L. REV. 813 (2001).

confronted with analogous technological constraints, unless users are technologically sophisticated, unauthorized uses are simply impossible. This is in fact where the potential savings from DRM accrues; because they curtail user discretion, technological barriers may be less costly for content owners to police and enforce. Consequently content owners may prefer to instantiate the terms of product use as computer code, rather than as contract or copyright law.

This disparity between legal and technical constraints stems in part from differences in the formulation of legal imperatives. Legal scholars have for some time engaged in a long-running debate over the comparative merits of so-called “rules” versus so-called “standards.”<sup>42</sup> Each of these types of legal imperative entails different costs and benefits, lending themselves to differing regulatory situations. Each type of imperative is characterized by its degree of determinacy, and the institution best suited to administer it. Perhaps most important to the distinction between these types of legal imperative is the point at which the legal imperative is created, and so the timing of cost incurred to properly formulate them.

“Rules” have been characterized as bright-line and definite decisional criteria.<sup>43</sup> Bright-line rules are typically designated before the occurrence to be regulated. Because they are simple and straightforward, rules are cheap to administer; the costs of their

---

<sup>42</sup> The body of literature on this topic is extensive. *See, e.g.*, Louis Kaplow, *Rules versus Standards: An Economic Analysis*, 42 DUKE L.J. 557 (1992); Duncan Kennedy, *Form and Substance in Private Law Adjudication*, 89 HARV. L. REV. 1685 (1976); Russell B. Korobkin, *Behavioral Analysis and Legal Form: Rules vs. Standards Revisited*, 79 OR. L. REV. 23 (2000); Eric A. Posner, *Standards, Rules, and Social Norms*, 21 Harv. J.L. & Pub. Pol’y 101 (1997); Frederick Schauer, *PLAYING BY THE RULES: A PHILOSOPHICAL EXAMINATION OF RULE-BASED DECISION-MAKING IN LAW AND IN LIFE* (1991); Pierre Schlag, *Rules and Standards*, 33 UCLA L. REV. 379 (1985); Cass R. Sunstein, *Problems With Rules*, 83 CAL. L. REV. 953 (1995).

<sup>43</sup> *See* Kaplow, *supra* note \_\_\_\_ at 559-560.

formulation will be incurred *ex ante*.<sup>44</sup> But because they are essentially predictive, designating precise behavior ahead of time, they are best formulated by an institution equipped to collect extensive predictive information, typically a legislature. Rules will tend to be favored where certainty is important, and decisional parameters can be most effectively determined on a comprehensive basis before they need to be applied.

Standards, by contrast, are characterized as flexible case-by-case decisional criteria that can take situational variance into account.<sup>45</sup> Standards operationalize case-by-case determinations by laying down a broad decisional criterion.<sup>46</sup> Such decisional flexibility necessarily vests a fair degree of discretion in a fact finder, typically the judiciary, in order to adapt the general imperative to the particular circumstance.<sup>47</sup> Because the precise application of the standard is determined after the fact, standards shift costs of administration to *ex post* decision-making.<sup>48</sup> Due to their flexibility and a priori indeterminacy, standards will be favored where the best outcome cannot be easily foreseen, and so determination after the fact is more efficient.

In addition to their respective benefits, each of these approaches entails certain drawbacks as well. Rules offer clear imperatives for behavior, but this means that they tend to be essentially binary; that is, one is either in compliance or one is not.<sup>49</sup> This in turn means that in their pure form, rules leave little room for nuance or factual shading. Due to their inflexibility, they may lead to costly outcomes if they fit a given situation

---

<sup>44</sup> *See id.*

<sup>45</sup> *See id.*

<sup>46</sup> *See id.* at 596; *see also* Isaac Ehrlich & Richard Posner, An Economic Analysis of Legal Rulemaking, 3 J. LEGAL STUD. 257, 278 (1974).

<sup>47</sup> Kathleen M. Sullivan, *The Justice of Rules and Standards*, 106 HARV. L. REV. 22 (1992).

<sup>48</sup> *See* Ehrlich & Posner, *supra* note \_\_\_ at 267.

<sup>49</sup> *See* Ronald M. Dworkin, *The Model of Rules*, 35 U. CHI L. REV. 14, 25 (1967)

poorly.<sup>50</sup> Exceptions to the rule, or excuses and justification for non-compliance, tend to make them look more like standards. Standards on the other hand tend to be fuzzier and more fact-dependent; because standards are typically and intentionally stated indeterminately, they offer little guidance as to expected behavior, and so may generate costs associated with this uncertainty.

For example, as I have indicated above<sup>51</sup>, access to creative works will tend to generate serendipitous and external benefits that are unlikely to be taken into account when setting the price and terms for usage. The inability to of purchasers, and hence of suppliers, to foresee such value militates in favor of standards-based determination of conduct; *ex ante* rule setting is no more likely to anticipate such value than are participants in the market. In contrast, an *ex post* evaluator can on a case-by-case basis take into account whatever benefit may have come from an unauthorized use. This standards-based approach is in fact characteristic of the user privileges under copyright, such as fair use, which involves a fact-specific balancing of the costs and benefits to a particular action after the action has occurred.

But because of their inherent limitations, regulatory designs are largely inimical to modeling standard-based decisions. Because the parameters of the desired behavior are incorporated into the design, regulatory design most closely resembles rule-based constraints.<sup>52</sup> As in the promulgation of legal rules, the costs of the constraint are incurred *ex ante*, as part of the design process; the anticipated behaviors and responses must be anticipated as the design is produced. It should come as no surprise that, as in the case of legal rules, the permissible range of behaviors is relatively sharply delineated,

---

<sup>50</sup> See Kaplow, *supra* note \_\_\_ at 596.

<sup>51</sup> See *supra* notes \_\_\_ and accompanying text.

relatively rigid, and insensitive to factual variation.<sup>53</sup> As in the case of the self-destructing DVD, situations unanticipated in formulating either rules or analogous designs will go unaccommodated by either type of constraint.

Despite the sophistication of the scripts incorporated into programmable technologies, this rule holds as true for DRM as for self-destructing DVDs or for speed bumps. Lacking the deliberative nuance of human agency, DRM lacks the flexibility to accommodate access or usage that is unforeseen, unexpected, or unanticipated.<sup>54</sup> Indeed, there is no incentive for the promulgators of DRM to even attempt to foresee usage with highly diffuse but positive social externalities: neither the copyright holder nor perhaps the purchaser of a copyrighted work not be the direct beneficiaries of such external effects, and so have no reason to take them into account. This in turn implies that technical protections will typically be unable to accommodate the many exemptions and exceptions to the copyright act, many of which are calibrated to capture just such benefits.

In previous work with Julie Cohen, I have shown that technological controls tend to be relatively blunt instruments for control of digital content, unable to accommodate copyright fair use without the re-introduction of human discretion.<sup>55</sup> Our suggestion for re-introducing human discretion into DRM has, with some justification been criticized,

---

<sup>52</sup> See Benoliel, *supra* note \_\_\_ at 1091 (2004).

<sup>53</sup> See *id.* at 1104.

<sup>54</sup> Contra 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* 597, 602-04 (Eberhard Becker et al. eds. 2003) (arguing that future DRM technologies will be sufficiently “malleable” to allow transformative reuses of protected content). The point that I have made here regarding the inability of DRM to accommodate legal standards, as underscored by Benoliel, *supra* note \_\_\_ and by Erickson & Mulligan, *supra* note \_\_\_, indicates why Bechtold’s assessment of future DRM is unduly rosy.

<sup>55</sup> See Dan L. Burk & Julie E. Cohen, *Fair Use Infrastructure for Copyright Management Systems*, 15 HARV. J. L & TECH. 41 (2001).

as essentially defeating DRM of much of its predictability, and so much of its benefit.<sup>56</sup> As I have shown here, it is the deterministic, bright-line predictability of DRM that makes it an attractive cost-saving mechanism *to the copyright holder*.<sup>57</sup> But as I have also shown, savings to the copyright owner are not the entirety of the social cost-benefit function. Locked into the rigid determinism of ex ante design decisions, DRM will also incur the social costs that would otherwise be minimized by the employment of legal standards. Any cost-benefit balance reflected in the array of rights privileges under the copyright statute is thus lost in technological substitution.

### **III. Technical Uniformity**

While the deterministic “scripting” of DRM accommodates only legal rules, rather than legal standards, it also drives DRM toward formation of technical uniformity, as the same ex ante design process that shapes DRM’s function shapes its technical character. The development promulgation of uniform technical characteristics, or technical standards, has been a topic of some considerable attention in the regulation of competition and in innovation policy.<sup>58</sup> That analysis is useful in the context of DRM promulgation as well, although the nature of DRM standards and their legal milieu raise heightened, possibly unique legal concerns.

“Standards” in this context, rather than referencing a type of legal imperative, may be defined as a set of technical specifications that provides common design features

---

<sup>56</sup> June Besek, *Anti-Circumvention Laws and Copyright: A Report from the Kernochan Center for Law, Media and the Arts*, 27 COLUM. J.L. & ARTS 385, 490-91 (2004).

<sup>57</sup> See Erickson & Mulligan, *supra* note \_\_\_\_.

for a product or process.<sup>59</sup> The potential benefits of uniform technical standards, and the problems attending incompatible standards, are commonplace knowledge.<sup>60</sup> As any traveler carrying an electrical appliance has discovered, the costs of non-uniform technical standards can be profound: voltage, current, and plug configuration vary enormously among different jurisdictions, requiring either expensive duplication of compatible appliances, or a panoply of adapters and transformers allowing a non-compatible appliance to interoperate with the local standards. Either compatibility strategy is cumbersome and costly. The ability of the same traveler to place a telephone call from nearly anywhere in the world to nearly anywhere else in the world speaks to the value of long-fought and hard-won compatibility in a different technology, telecommunications.

In each case of compatibility or incompatibility, this standardization problem is intimately tied to the costs and benefits of network effects. Network effects may arise in situations where the value of a system increases as users are added.<sup>61</sup> Purchasers of network goods find the good increasingly valuable as others also purchase the good. Typically, the increased value accrues to subsequent adopters, and accrues as a positive externality.<sup>62</sup> For example, a telephone system is of relatively little value if it has only

---

<sup>58</sup> See Sean P. Gates, *Standards, Innovation, and Antitrust: Integrating Innovation Concerns into the Analysis of Collaborative Standard Setting*, 47 EMORY L.J. 583 (1998); James J. Anton & Dennis A. Yao, *Standard-Setting Consortia, Anti-Trust, and High Technology Industries*, 64 ANTITRUST L.J. 247 (1995).

<sup>59</sup> 2 HERBERT HOVENKAMP ET AL., IP AND ANTITRUST: AN ANALYSIS OF ANTITRUST PRINCIPLES APPLIED TO INTELLECTUAL PROPERTY LAW § 35.1 at 35-3 (2002).

<sup>60</sup> See CARL SHAPIRO & HAL R. VARIAN, INFORMATION RULES 229 (1999).

<sup>61</sup> See Michael L. Katz & Carl Shapiro, *Network Externalities, Competition, and Compatibility*, 75 AM. ECON. REV. 424 (1985).

<sup>62</sup> See S.J. Liebowitz & Stephen E. Margolis, *Network Externality: An Uncommon Tragedy*, 8 J. ECON. PERSP. 133, 135 (1994) (distinguishing between positive and negative network effects).

two subscribers; each subscriber can call only one other person.<sup>63</sup> The system is of greater value if it has more subscribers, because each subscriber can then communicate with many others. Those who subscribe to the system after it has accrued a large number of subscribers may obtain a more valuable service than those who subscribed early, when there were few other subscribers. At the same time, the value of the service to the early subscribers grows as additional users sign on to the network.

This insight can be generalized to other types of human artifacts with shared compatibility; languages, for example, may be thought of as goods having network effects. The ability to “interoperate” internationally with a wide diversity of individuals is illustrated by the benefits of speaking Greek in the ancient Western world, Latin in the Medieval Western world, or English in the current global era. As another well-studied example and pertinent example, many commentators have noted that computer operating systems tend toward a uniform standard because of the natural benefits of a uniform standard: users need only invest in learning the characteristics of the system once, technical support for a single standard is simple to provide, and producers of compatible software applications need only develop products to function with a single platform.

The Internet, for example, is a prime candidate for display of such network externalities: network access becomes more valuable as it becomes more ubiquitous.<sup>64</sup> Much of the success of the Internet itself is due to the creation of a new type of physical network: the internetworking protocols on which the Internet operates allow disparate types of computer hardware, running many different software systems, to interact on a

---

<sup>63</sup> See Katz & Shapiro, *supra* note \_\_ at 424 (citing telephones as an example of network effects); Liebowitz & Margolis, *supra* note \_\_ at 139-40 (noting the telephone system as a paradigmatic example of network effects).

single network. Thus, users with previously incompatible equipment can now join the same system and interoperate. Additionally, any given application run on the network may show a different kind of network effect from usage: e-mail, for example, is a more valuable service if it can be used more widely. Similarly, the World Wide Web software application becomes more valuable as it accumulates more reference linkages, allowing more information to be indexed and accessed.

Both types of network activities are simultaneously possible because the Internet exhibits more than one type of network effect. Katz & Shapiro have distinguished between these effects as actual and virtual networks.<sup>65</sup> Actual networks may be characterized as those that physically interoperate with one another; virtual networks as those that share common features without direct interoperation. To the extent that a system shares a technical configuration that allows machines to physically interconnect, it represents an actual network. Whereas the benefits accruing from similarity of software platforms or, for that matter, from the content on the system, comprise a virtual network of shared compatibility. Where a common technical standard is available, both types of beneficial effects may be generated.<sup>66</sup>

At the same time, there exists a serious potential downside for any standards setting process. Networks may also produce negative effects, as the cost of leaving the network, even when it would be socially desirable to do so, may be prohibitively high.<sup>67</sup>

---

<sup>64</sup> See Mark A. Lemley, *Antitrust and the Internet Standardization Problem*, 28 CONN. L. REV. 1041 (1996).

<sup>65</sup> See Michael L. Katz & Carl Shapiro, *Systems Competition and Network Effects*, 8 J. ECON PERSP. 93, 95 (1994).

<sup>66</sup> See Carl Shapiro, *Setting Compatibility Standards: Cooperation or Collusion?* in EXPANDING THE BOUNDARIES OF INTELLECTUAL PROPERTY: INNOVATION POLICY FOR THE KNOWLEDGE SOCIETY 81, 88 (Rochelle Cooper Dreyfuss et al eds., 2001).

<sup>67</sup> See Mark A. Lemley & David McGowan, *Legal Implications of Network Economic Effects*, 86 CAL. L. REV. 479, 551 (1998).

The likelihood of “lock-in” to an inefficient standard remains a disputed, but nonetheless serious consideration.<sup>68</sup> The concern in such situations is that once a standard is adopted, network effects may raise the cost of changing to a newer or better alternative causing the standard to become permanently entrenched. This may possibly occur where the short-term costs of switching away from the old standard are greater than the long-term benefits of the new standard – indeed, it has been argued that development of new standards may be deterred if network effects raise the short-term cost of development and deployment of the new standard above the perceived savings of a new standard.

But because standard-setting is often beneficial, and indeed may be critically important where network efficiencies can be realized development of standards is generally desirable, and facilitated by a variety of mechanisms.<sup>69</sup> In some cases, the government may formally mandate a standard. In other cases, actors in an industry may voluntarily band together to settle on a standard; this may occur through informal consultations or under the auspices of a more formal standards setting organization. In yet other cases, a *de facto* standard may arise spontaneously, for example in an industry where a particular product configuration or characteristic evolves to dominance.

In each of these cases, the development of standards carries potential risks to competition, related to the potential negative consequences of network effects. Most such concerns relate to anti-competitive manipulation of the standards-setting process, or the standard itself, to achieve some form of market dominance.<sup>70</sup> Private standard-setting

---

<sup>68</sup> See S.J. Leibowitz & Stephen E. Margolis, *Network Externality: An Uncommon Tragedy*, 8 J. ECON. PERSP. No. 2, at 133 (1994); S.J. Leibowitz & Stephen E. Margolis, *The Fable of the Keys*, 33 J.L. & ECON. 1 (1990).

<sup>69</sup> See Mark A. Lemley, *Intellectual Property Rights and Standard-Setting Organizations*, 90 CALIF. L. REV. 1889 (2002).

<sup>70</sup> See Stanley M. Besen & Joseph Farrell, *Choosing How to Compete: Strategies & Tactics in Standardization*, 8 J. ECON. PERSP. 117 (1994).

organizations, for example, may sometimes cloak anticompetitive cartel-like activity if their membership is limited and conditions permit them to control adoption of the standard. Closed standard-setting organizations might prevent non-member competitors from participating in determination of an industry standard, and perhaps more importantly, may prevent non-members from licensing proprietary technologies incorporated into a standard. Even outside an organizational setting, it has been argued that a dominant industry player may be able to arrange “tipping” of the market toward a desired standard; presumably, a proprietary standard that can be controlled or exploited. Concern in this regard has been particularly keen where the standard that is adopted, or which evolves to dominance, is covered by patent, copyright, or similar exclusive rights.

Like other computer technologies, DRM will be shaped by network effects, and can be expected to converge on a standard. Indeed, as a practical matter, DRM will only work if all the publishers in a relevant industry agree to employ it – otherwise, unauthorized copies will quickly become available and proliferate from unprotected sources. As DRM becomes ubiquitous, consumers and users of DRM and DRM protected content can be expected to seek the convenience and savings of compatible devices and file formats. In some instances, industry groups such as the DVD consortium have already developed DRM and DRM compatible standards for particular media.<sup>71</sup> In other areas, such as digital music, industry development of such standards has been an elusive goal, and the lack of compatibility and interoperability between differing rights-managed music formats has been a source of frustration to consumers.

DRM constraints themselves constitute a type of levy price increase on the value of creative works – users who are accustomed to unimpeded access to copyrighted works

will be hampered in using what they have purchased. – the convenience of playing music or movies on different types of equipment, the value of transferring content to an automobile or portable playback system, and so on. Substantial DRM interference with consumer use of the work effectively makes the work “overpriced,” potentially causing consumers to complain, to switch their buying to other, less obnoxious, forms of entertainment, or to switch to alternative versions of the same content – depending on the comparative annoyance costs, perhaps borrowed from friends, obtained from a library, or downloaded from an unauthorized file-sharing source. Publishers will of course have some incentive to assess and accommodate value that users derive from some types of unimpeded access. As I have suggested above, it is unclear that the publishers of technically protected content are in a good position to assess such uses *ex ante*, and costs not internalized by consumers, and so not taken into account by publishers, remain a social welfare concern. But diminution of the value of the content due to DRM may provide some degree of market discipline, as publishers with the least intrusive DRM, or perhaps those willing to forgo DRM, capture market share from others whose DRM configurations restrict the value of their content to consumers.

Consequently, while development of DRM standards carries with it the usual concerns over network “lock-in,” cartel behavior, and market “tipping,” many of the natural market safeguards against monopoly pricing, such as new entry, should also apply: for example, defectors from such an industry-wide DRM agreement might reap the rewards of lower annoyance costs, at least in the short term, at the expense of competitors employing DRM. But in the case of DRM, an additional set of considerations heightens and exacerbates the usual concerns over anti-competitive conduct. These concerns relate

---

<sup>71</sup> See Bechtold, *supra* note \_\_\_\_ at 631-37.

to the security of interoperable standards themselves. The use of digital media requires the interoperation of a variety of software and hardware devices. Content files do not exist in isolation, but require devices to read and translate the files to output, to move files between different locations in the computer, to copy the files to different formats within the computer, and to perform a variety of other operations. But because the security of rights-managed content might be compromised by interaction with devices that are not themselves secured, dependable rights management requires some form of protection or safeguard against insecure devices.<sup>72</sup>

The most secure approach is to simply decline or prohibit interoperation with potentially insecure devices. Consequently, developers of rights management systems have proposed the creation of trusted platforms that in essence generate a secure perimeter for interoperation, and allow within that perimeter only those devices judged to be safe.<sup>73</sup> In proposed systems such as Microsoft's secure platform, formerly known as "Palladium," the central processor of the computer, as the computer boots up, would systematically examine, authenticate, and certify devices attached to the system -- that is to say, that the processor would allow interaction only with devices that were recognized as being secure.<sup>74</sup> Interaction with devices that are not recognized, or that were deemed to be insecure, would be declined. Under this approach the security concerns or "trust management" protocols of DRM dictates the exclusion of devices that are technically compatible, but untrusted.

---

<sup>72</sup> See Jonathan Weinberg, Hardware-Based ID, Rights Management, and Trusted Systems in THE COMMODIFICATION OF INFORMATION 343 345-46 (Niva Elkin-Koren & Neil W. Netanel, eds. 2002).

<sup>73</sup> See generally SIANI PEARSON, TRUSTED COMPUTING PLATFORMS (2003).

<sup>74</sup> See Bechtold, *supra* note \_\_\_ at 638-39; Ross Anderson, TCPA/Palladium Frequently Asked Questions, <http://www.cl.cam.ac.uk/rja14/tcpa-faq.html>

As secured machines are networked, this strategy extends to trusted content and rights management systems operating over the Internet or similar computer networks.<sup>75</sup> The design of such distributed systems calls for secure servers that would provide remote users with access to or content from data and entertainment archives, but only on recognition of trusted technical safeguards.<sup>76</sup> Archived content would be packaged with pre-determined DRM controls instantiating the usage limitations specified by the owner. On-line requests for access to content, or for purchase and download of content, would be honored only where the recipient machine was certified as capable of securely implement the bundled DRM. Thus, the DRM protocols for automated acquisition of creative works, too, would dictate exclusion of technically compatible but untrusted devices.

In a secured, rights-managed environment, therefore, interoperation and the ability to produce viable interoperative products depend not only on the standard for technical compatibility, but on the standard for defining and implementing “trust.”<sup>77</sup> A full discussion of the technical and operational parameters of trust management lie well beyond the scope of this paper<sup>78</sup>, but since security is never absolute, such parameters are not necessarily objective in all dimensions, requiring at minimum a judgment as to how secure is secure enough. Where interoperation is at issue, the potential for considerable anti-competitive mischief may lie in such judgments; one can well imagine the possessor of a dominant market position protecting that position by excluding rival products from interoperation, ostensibly on security concerns, but clandestinely on strategic criteria.<sup>79</sup>

---

<sup>75</sup> See Weinberg, *supra* note \_\_\_\_ .

<sup>76</sup> See Bechtold, *supra* note \_\_\_\_ at 639-41.

<sup>77</sup> See generally Batya Friedman et al., *Trust Online*, 43 COMM. ACM 34 (2000).

<sup>78</sup> For thorough treatments, see generally L. JEAN CAMP, TRUST AND RISK IN INTERNET COMMERCE (2000); COMMITTEE ON INFORMATION SYSTEMS TRUSTWORTHINESS, NAT'L RESEARCH COUNCIL, TRUST IN CYBERSPACE (1999).

<sup>79</sup> See Bechtold, *supra* note \_\_\_\_ at 641-42.

Even if the alleged security concerns leading to exclusion are wholly legitimate, concealing no illegitimate anti-competitive motivation, the practical effect of the exclusion may be the same, barring entry to innovative complementary or competing products.

Of course, trust management exclusion is difficult if the technical criteria for interoperation are known; competitors may simply design their products to meet the technical standard and enter the market regardless. This can be expected in an open market, and helps serve as a check on many types of exclusive design strategies. DRM may be designed to monitor and enforce its own trust criteria but such safeguards can themselves be designed around. However, if legitimate competitors can design around the technical safeguards against untrusted interoperation, so may technicians with more nefarious goals in mind. By the same token, sheltering or concealing the criteria of a technical security standard stymies not only illegitimate attempts at access, but legitimate ones. This double-edged result of standard suppression threatens normal market corrections that depend upon the accessibility to DRM protocols. In particular, the ability of new entrants or other competitors to gain unconsented access to technical protocols necessary for interoperation has been greatly complicated by a legal regime enacted to reinforce the security of DRM technologies.

#### **IV. Anti-Circumvention Law**

I have argued above that, while design constraints and legal constraints are to some extent interchangeable, these two substitutes may engage in complex interaction:

the two may complement and re-enforce one another.<sup>80</sup> The state may promulgate rules requiring manufacturers to install seatbelt ignition interlocks, or may assign liability in such a way as to induce their installation, but may also promulgate laws penalizing consumers who disable the interlocks, in order to ensure that the regulatory device has the intended effect. The same interrelationship holds true for DRM. While proposals to require or induce use of DRM have not thus far been adopted<sup>81</sup>, laws reinforcing the voluntary deployment of DRM have been.

The rationale behind such laws maintains that where technology provides the first line of defense against unauthorized uses of copyrighted works, the legal protection needed to encourage creativity may be not so much a deterrent against violation of copyright or similar proprietary rights, but legal deterrents against circumvention of technological protections.<sup>82</sup> In the United States, a legal deterrent of this kind has been enacted in the form of the Digital Millennium Copyright Act, or DMCA, which prohibits circumvention of technical protection measures, and trafficking in technology that would facilitate such circumvention.<sup>83</sup> This statute effectively provides content owners a new right of technological access, independent of any intellectual property right. Language promulgating similar legal measures has appeared in a recent European Union Copyright directive.<sup>84</sup>

---

<sup>80</sup> See *supra* notes \_\_\_ and accompanying text.

<sup>81</sup> See, e.g., S. 2048, 107<sup>th</sup> Cong. (2002) (unenacted "Security Systems Standards and Certification Act"); see also Bechtold, *supra* note \_\_\_ at 651-52.

<sup>82</sup> See Eric Schlachter, *The Intellectual Property Renaissance in Cyberspace: Why Copyright Law Could Be Unimportant on the Internet*, 12 BERKELEY TECH. L.J. 15 (1997).

<sup>83</sup> Digital Millennium Copyright Act, Pub. L. No. 105-304, 112 Stat. 2860 (1998).

<sup>84</sup> Directive 2001/29/EC of the European Parliament and of the Council of 22 May 2001 on the harmonization of certain aspects of copyright and related rights in the information society, 2001 Q.J. (L. 167) 10.

In the United States, the statute was touted as legislation necessary to fulfill the United States' obligations under the World Intellectual Property Organization Copyright Treaty (WIPO Treaty).<sup>85</sup> However, the treaty requires only that signatory states provide "adequate legal protection and effective legal remedies" against circumvention of technological controls.<sup>86</sup> In the United States, such protection would already have been provided under the doctrine of contributory infringement, which attributes copyright liability to providers of technical devices that lack a substantial non-infringing use.<sup>87</sup> This provision of U.S. law could have been employed against provision of so-called "black box" devices intended to circumvent technological protections. The compliance of U.S. law with the requirements of the treaty was so substantial that the Clinton administration initially considered submitting the WIPO treaty to the Senate for ratification without accompanying implementing legislation.<sup>88</sup>

Instead, lobbying by content industries resulted in the enactment of so-called "implementing" legislation containing anti-circumvention provisions that far exceed anything contemplated by the treaty.<sup>89</sup> Starkly put, the DMCA as enacted creates a new and unprecedented right to control access to copyrighted works. The statute outlaws the act of circumventing "a technological measure that effectively controls access to a work protected under this title."<sup>90</sup> It also prohibits "trafficking" or providing the means to circumvent either technological access controls or technological measures that control the

---

<sup>85</sup> See Pamela Samuelson, *The U.S. Digital Agenda at WIPO*, 37 VA J. INT'L L. 369, (1997).

<sup>86</sup> World Intellectual Property Organization: Copyright Treaty, December 20, 1996, art. 11, 36 I.L.M. 65

<sup>87</sup> See *Sony v. Universal Studios*, 464 U.S. 417 (1984).

<sup>88</sup> See Pamela Samuelson, *Intellectual Property and the Digital Economy: Why the Anti-Circumvention Regulations Need to Be Revised*, 14 BERKELEY TECH. L.J. 539 (1999).

<sup>89</sup> Indeed, the DMCA anti-circumvention provisions contain language very close to that rejected by the treaty Diplomatic Conference as overbroad and detrimental to the public domain. See Samuelson, *supra* note \_\_\_ at 413-15.

<sup>90</sup> 17 U.S.C. § 1201 (a)(1)(A)

exclusive rights of a copyright holder: that is to say, copy controls, display or performance controls, and so on. Congress appears to have distinguished between access controls and usage controls, allowing circumvention of the former but not the latter, in order to enable user privileges and exemptions.<sup>91</sup> In theory, a user would have to obtain authorized access to a protected work, but having done so, could without authorization circumvent usage controls to make fair or other permissible uses. In reality, however, few content users have the skills to circumvent the usage controls, and the statute prohibits those who have such skills from assisting those who do not. Moreover, access controls are essentially indistinguishable from usage controls, and essentially provide control of both access and use.<sup>92</sup>

The act provides for a handful of exceptions for purposes such as law enforcement, encryption research, and security testing. The statutory exceptions are confusing and somewhat contradictory, but are primarily directed to the prohibition on circumvention; exceptions to providing circumvention means are extremely limited. First, the Librarian of Congress is empowered under the statute to periodically exempt certain classes of works from the prohibition on access circumvention in order to preserve selected access for socially valuable non-infringing uses.<sup>93</sup> Additionally, the statute incorporates several standing exceptions to the access prohibition. Circumvention of technological controls is permitted for legitimate governmental intelligence and law

---

<sup>91</sup> See R. Anthony Reese, *Will Merging Access Controls and Rights Controls Undermine the Structure of Anticircumvention Law?*, 18 BERKELEY TECH. L.J. 619 (2003).

<sup>92</sup> See, e.g., *Universal Studios v. Remeirdes* 111 F.Supp.2d 294 (S.D.N.Y. 2000) (classifying the CSS technological control system for DVDs as both an access control and a usage control.)

<sup>93</sup> 17 U.S.C. § 1201 (a)(1)(B)-(D). In the first such rule-making, which the Librarian delegated to the Register of Copyrights, consideration of exemptions was limited to situations in which actual harm from the inability to circumvent could already be shown. Consequently, only two exemptions were granted, the first for circumvention of access controls on works where the technological measures had malfunctioned,

enforcement purposes.<sup>94</sup> Nonprofit library and educational institutions may circumvent in order to make a good faith determination whether to acquire a copy of the protected work.<sup>95</sup> Circumvention is also permitted in order for software developers to achieve interoperability among computer products<sup>96</sup>, for encryption research<sup>97</sup>, and to test computer security.<sup>98</sup> Parents may circumvent in order to prevent their children from accessing harmful content on the Internet.<sup>99</sup> Individuals may circumvent in order to protect the privacy of their “online activities.”<sup>100</sup> The act also incorporates statements that digital equipment manufacturers are under no affirmative duty to design their products to accommodate particular content control systems<sup>101</sup>; that the anticircumvention provisions are not intended to alter copyright remedies, limitation, and defenses such as fair use<sup>102</sup> or to broaden contributory or vicarious copyright liability<sup>103</sup>, or to enlarge or diminish rights of free speech or press activities involving consumer electronics, telecommunications, or computing products.<sup>104</sup>

The DMCA anti-circumvention device provisions are directed to two different types of technological measure. The first is directed to devices that circumvent technological measures that control access to a copyrighted work.<sup>105</sup> The second is directed to devices that circumvent technological measures that protect the rights of a

---

and a second for parents to access the list of restricted sites in Internet filtering software. *See* 37 C.F.R. § 201.40.

<sup>94</sup> 17 U.S.C. § 1201 (e).

<sup>95</sup> § 1201 (d).

<sup>96</sup> § 1201 (f).

<sup>97</sup> § 1201 (g).

<sup>98</sup> § 1201 (j).

<sup>99</sup> § 1201 (h).

<sup>100</sup> § 1201 (i).

<sup>101</sup> § 1201 (c)(3)

<sup>102</sup> § 1201 (c)(1)

<sup>103</sup> § 1201 (c)(2)

<sup>104</sup> § 1201 (c)(4)

<sup>105</sup> § 1201 (a)(2)

copyright holder in a work or portion of a work.<sup>106</sup> Each provision prohibits the manufacture, importation, provision, public offering, or trafficking in a technology, product, service, device, component, or part thereof if primarily designed or produced for the purpose of circumventing, has only limited commercially significant purposes or use other than to circumvent, or is knowingly marketed for use in circumvention.<sup>107</sup>

These device provisions are subject to confusing and contradictory exceptions that are narrower than the seven exceptions to the provision prohibiting acts of circumvention. Circumvention devices necessary for interoperability are privileged<sup>108</sup>, but devices for law enforcement and privacy reasons are not. Devices necessary to circumvent access controls are privileged for encryption and for security research<sup>109</sup>, but devices to circumvent rights controls for the same purposes are not. There is no provision for devices necessary to gain access or circumvent rights controls in order to make fair use or other uses permissible under the copyright act, despite the statements in the Act that it was not intended to alter such privileges.<sup>110</sup>

This apparent inflexibility in the statute should perhaps be unsurprising. The purpose of backing the integrity of technical controls by statute is to shift enforcement of the rights-holder's interest from penalties for unauthorized infringement to penalties for unauthorized access. Given that DRM is only able to channel user conduct into dependably secure behaviors when its architecture is predictable and deterministic, the legal imperatives that guard the technical controls must be equally predictable and deterministic. Just as technical regulation under DRM cannot accommodate the fact-

---

<sup>106</sup> § 1201 (b)(1)

<sup>107</sup> § 1201 (a)(2)(A)-(C); (b)(1)(A)-(C).

<sup>108</sup> § 1201 (f)(2)

<sup>109</sup> § 1201 (g)(4), (j)(4).

dependent, ex ante flexibility of legal standards, so the accompanying legal regulation of circumvention resists such situational flexibility.

By adopting ex ante, deterministic, legal imperatives, anti-circumvention laws, acting as an adjunct to deterministic technological controls, confer upon content owners a degree of control over creative works never attainable under a regime of traditional copyright.<sup>110</sup> The rule-based approach assumes that both Congress and copyright holders can determine ex ante the proper balance of cost and benefit, but as described previously, whenever unforeseen or unanticipated costs arise, a rules-based approach will fail to properly calibrate behavior. One potential result of the DMCA approach, unaccounted for in the calculus of creative incentives, may be that this combination of legal and technical control drives the promulgation of monolithic DRM technical standards: by deterring legitimate circumvention of DRM, the DMCA provisions help to “lock in” the dominant technical standard by frustrating interoperation or replacement by competing products. Thus, unprecedented control over content potentially confers unprecedented market power on the developer of the dominant technical standard, facilitating anti-competitive conduct.

## **V. Anti-Competitive Applications**

The potential for the DMCA anti-circumvention provisions to foster anti-competitive conduct has already become apparent. In the relatively short time since their

---

<sup>110</sup> 17 U.S.C. § 1201 (c)(1), (c)(2).

<sup>111</sup> Cf. Jane Ginsburg, *Copyright and Control*, 101 COLUMB. L. REV. (2001) (arguing that emergence of new technology may justify granting copyright owners a higher degree of control over works); Jane

enactment, the DMCA anticircumvention provisions have been invoked in a handful of cases and reported incidents. Courts have typically been sympathetic to such claims when the incidents have reached the point of judicial action, although recent appellate opinions may signal a shift toward greater skepticism over DMCA claims. This shift may stem from a pattern of litigation in which misappropriation of technically protected content is seldom present, suppression of competitive products seems a likely motivation, and the claims brought have become increasingly divorced from the entertainment piracy that Congress initially intended to deter by passage of the DMCA.

The earliest cases asserted under the anti-circumvention statutes bore at least a nominal connection to entertainment piracy, although the issue of control over non-entertainment products was never far distant. in *Universal City Studios v. Reimerdes*.<sup>112</sup> The *Reimerdes* suit was based upon circumvention of a technical control system known as the Content Scrambling System, or CSS, which was designed to secure access to DVD movie discs.<sup>113</sup> A key feature of the system was that the software controls embedded in the disc allowed discs to be played only on approved consumer playback machines.<sup>114</sup> Machines manufactured in different geographic areas were designed to allow access to the content of a given DVD only if the disc was coded to be played in that in corresponding geographic area, thus allowing significant control over the timing and distribution of movies released in different parts of the globe. The corollary to this technological control system is that DVDs may only be played on approved playback

---

Ginsburg, *From Having Copies to Experiencing Works* in US INTELLECTUAL PROPERTY: LAW & POLICY (Hugh Hansen ed. 2000) (same).

<sup>112</sup> 82 F. Supp. 211 (S.D.N.Y. 2000) *aff'd sub nom* Universal City Studio v. Corley, 273 F.3d 429 (2d Cir. 2001).

<sup>113</sup> *Id.* at 214.

<sup>114</sup> 111 F.Supp.2d 294, 308 (S.D.N.Y. 2000).

equipment, whose manufacturer has built the equipment for use with the control system.<sup>115</sup>

In response to this limitation, a fifteen year old Norwegian youth developed a program that he called “DeCSS,” designed to circumvent the access controls, purportedly in order to allow DVDs to be played on non-approved playback systems.<sup>116</sup> Use of the DeCSS program would thus allow DVDs purchased in one area of the world to be played on equipment that would otherwise be geographically incompatible. It would also allow DVDs to be played on unapproved playback equipment, and in particular, allow the discs to be played on a Linux operating system platform, for which no approved device existed.<sup>117</sup> The owners of DVD content – which is to say, movie studios – alleged that the DeCSS “hacking tool” violated the DMCA provisions prohibiting trafficking in circumvention devices, and successfully filed suit to prevent various web sites from either directly distributing the program or offering hypertext links to other sites where it might be found.<sup>118</sup> Both the district court and the appellate court hearing the case rejected any claim that the First Amendment might privilege distribution of DeCSS computer code, or that owners of DVDs might be entitled to such a tool in order to engage in fair use. The court determined instead that Congress had intended to create a new form of protection for technologically secured works, and had no obligation to ensure that this new statutory scheme accommodated consumers in exercising their fair use under copyright law.

---

<sup>115</sup> *Id.*

<sup>116</sup> *Id.* at 311.

<sup>117</sup> *Id.*

<sup>118</sup> 82 F.Supp.2d 211.

While the DMCA claims brought in *Remierdes* were ostensibly advanced to protect the integrity of movies from unauthorized duplication, the practical outcome was that DVD movie playback remained tied to approved systems – effectively controlling a market for consumer electronics that was well beyond the intellectual property interest in copyrighted movies. Control over interoperable technology, rather than an explosion of unauthorized copying, seemed similarly at the heart of the DMCA dispute in *RealNetworks v. Streambox*<sup>119</sup>, a DMCA action brought by the publisher of a popular software package used to receive music or video “streams” via the Internet. The RealPlayer receiver software, which would be typically installed on a user’s desktop machine, achieves connection with a RealPlayer music or video server elsewhere on the network through a “secret handshake” protocol that allows the server and receiver to recognize one another.<sup>120</sup> Once a connection is achieved, the system contains a feature to determine whether the user of the receiver has obtained rights to copy the music files sent by the server, or only to listen to the music as it is sent.<sup>121</sup>

The defendant Streambox produced a competing receiver, as well as several other pieces of software designed to be interoperable with the RealPlayer system. In order to play RealPlayer signals, the Streambox receiving components connected with the RealPlayer server by emulating the “secret handshake” protocol.<sup>122</sup> However, once the connection was established, the Streambox product lacked the restriction feature that would prevent unauthorized copying of streamed music or video. RealNetworks brought suit against Streambox, alleging that their receiving components constituted a

---

<sup>119</sup> No. C99-2070P (W.D. Wash. Jan. 18, 2000), 2000 U.S. Dist. LEXIS 1889.

<sup>120</sup> 2000 U.S. Dist LEXIS 1889 at \*6.

<sup>121</sup> *Id.*

<sup>122</sup> *Id.* at \*11.

“circumvention device” under the DMCA. In an unpublished opinion, the court granted the preliminary injunction, holding that the emulation of the “secret handshake” protocol constituted a circumvention of the RealPlayer restriction features.<sup>123</sup>

The most striking feature of this opinion is that no content owner appears – although the DMCA was purportedly enacted to protect owners of copyrighted content, in the *RealNetworks* case, only producers of competing software technology were involved. No pirating or unauthorized reproduction of any copyrighted content was shown, only the production of an interoperable product that could have been used to produce unauthorized copies of content. At least one way to view the facts is as an attempt by a software publisher to impede or abolish the distribution of a rival product, and at a minimum the case demonstrates that the statute could be turned to such purposes.

Subsequent DMCA cases have moved yet farther away from claims related to copyright piracy, instead asserting anticircumvention claims where unapproved uses of copyrighted works might disrupt the producer's preferred marketing scheme – a problem seen in *Reimerdes*, but having many other incarnations. For example, in *Sony v. Game Masters*<sup>124</sup>, the alleged circumvention device was an add-on module to the PlayStation videogame console. The device, called a “Game Enhancer” could be used to speed up or increase the difficulty of Sony games. But the devices was also sold with instructions on how use a U.S. marketed console to play games intended for sale only in Europe or Japan.<sup>125</sup> Much like of the DVD CSS territory codes in *Reimerdes*, the PlayStation console was designed to operate when encrypted data from a game CD verified that the game was a Sony produce authorized for distribution in the same geographical territory

---

<sup>123</sup> *Id.* at \*19-20.

<sup>124</sup> 87 F.Supp.2d 976 (1999).

as the console. The instructions allowed players to initialize a U.S. game, then temporarily turn control of the console over to the Game Enhancer while the U.S. game was removed and an import game inserted and loaded.<sup>126</sup> Control was then turned back over to the console's operating system, which would execute the game software based on the previous authorization. The court concluded that this constituted circumvention of a technological measure in violation of the DMCA, and that distribution of the Game Enhancer violated the DMCA trafficking provisions.<sup>127</sup>

The anti-circumvention claims in *Game Masters* were intended to suppress the use of lawfully purchased game cartridges in a manner contrary to the copyright holder's wishes. Control over post-purchase use of legitimate software was similarly at issue in the DMCA claims brought in *Davidson & Associates v. Internet Gateway*.<sup>128</sup> The plaintiff, Blizzard Entertainment, is the publishers of a variety of popular computer video games, whose games include a "multi-player mode" that would allow players to play against one another by means of the Internet. This online multi-player service, called Battle.net, authenticated players by means of an encrypted "secret handshake"<sup>129</sup> sequence. When game users log onto Battle.net, the service requests the authentication sequence that accompanied a purchased game. If the sequence given was recognized as belonging to a purchased game, and was not already in play, the service would permit access.

The defendants in the case were the volunteer developers of an alternative, open source network, called the "bnetd" project, which was intended to offer the same

---

<sup>125</sup> *Id.* at 981.

<sup>126</sup> *Id.* at 981-82.

<sup>127</sup> *Id.* at 987.

<sup>128</sup> 2004 U.S. Dist. LEXIS 20369 (E.D. Mo. Sept. 30, 2004)

experience as Battle.net, but avoid certain difficulties or objectionable materials users experienced on Battle.net. Like Battle.net, the bnetd software would allow Blizzard game players to interact in multi-player mode over the Internet. In order to allow players to interact in multi-player mode, it was necessary for the bnetd developers to reverse engineer Blizzard software and protocols.<sup>130</sup> It was also necessary for the bnetd system to interact with the individual game software modules via the “secret handshake” protocol, although bnetd was not designed to check the game sequence to determine if the sequence belonged to a purchased game or was not already in play.

Blizzard sued the bnetd developers for anticircumvention violations. Relying on previous decisions such as *Gamemasters*, the district court found the developers to be trafficking in access circumvention tools that gave unauthorized access to the Battle.net mode of the games.<sup>131</sup> The court rejected the notion that the access users of the bnetd system, who were lawful purchasers of the Blizzard games, were engaged in authorized access by virtue of owning the games; the court was convinced instead that the owners of the games lacked lawful permission to circumvent the Battle.net technical protections. Similarly, the court decided that the DMCA reverse engineering exception did not apply, because the bnetd developers were not seeking interoperability of an “independently created computer program,” but rather to produce a substitute for Battle.net. Such a substitute product was held not to be a legitimate object for the reverse engineering exception.

The use of the anti-circumvention provisions to exclude from the marketplace not threats to the technical protection of a copyrighted product, but interoperable products

---

<sup>129</sup> *Id.* at \*10.

<sup>130</sup> *Id.* at \*21.

that might disturb copyright holder's plans for an adjacent market, is troubling. But by far the most egregious employment of the DMCA has been to block the sale of competing products in consumer devices with no relationship whatsoever to copyright piracy. A claim of this sort was brought in *Lexmark Int'l Inc. v. Static Control Components Inc.*<sup>132</sup>, where a manufacturer of computer printers filed a DMCA circumvention infringement suit against the manufacturer of computer chips incorporated into competing new or refilled ink cartridges.<sup>133</sup> Lexmark, a major computer printer manufacturer, sells both printers and ink toner cartridges. The cartridges are recognized by the printer via a software authentication sequence programmed into a chip in the cartridge.<sup>134</sup> Rival manufacturers' refilled aftermarket cartridges would not function with the printer unless they mimicked this sequence.<sup>135</sup> The trial court held that by providing chips that allow rival cartridges to be recognized by the printer, defendant Static Control was trafficking in a tool circumventing a technological measure, because the program in the cartridge chip "controlled access" to the printer software.<sup>136</sup> The trial court also rejected the defendant's defense under the reverse engineering provisions of the DMCA, holding that the accused devices comprised "independently created computer program," but only copies of the Lexmark printer control programs.<sup>137</sup> The trial court also case expressly rejected the suggestion that the DMCA provisions were targeted against copyright piracy,<sup>138</sup> reasoning that this goal would have been accomplished by the

---

<sup>131</sup> *Id.* at \*54.

<sup>132</sup> 253 F. Supp. 2d 943 (E.D. Ky. 2003).

<sup>133</sup> *Id.* at 947.

<sup>134</sup> *Id.* at 952.

<sup>135</sup> *Id.* at 952-53.

<sup>136</sup> *Id.* at 969.

<sup>137</sup> *Id.* at 971.

<sup>138</sup> *Id.* at 968.

DMCA usage circumvention provisions, rendering the access provisions “surplussage.”<sup>139</sup>

Similar anticircumvention claims have also been asserted over the interoperability of garage door openers, a product perhaps even farther removed from entertainment copyright piracy than printer ink cartridges. In *Chamberlain v. Skylink*, the plaintiff, a manufacturer of garage door opening equipment, attempted to exclude from the market “universal” remote control units that were designed to function as a back-up or replacement remote control for its own remote control devices. The Chamberlain remote control used a rolling code, that would shift from use to use, purportedly in order to avoid the possibility that a burglar might capture the code beamed from the remote control and use the captured code to open the garage door, allowing unauthorized entry to the home. In order to interoperate with the door opening mechanism, the Skylink universal remote was developed to the rolling code. Chamberlain sued, claiming that the Skylink devices circumvented a technical measure that protected the security code.

But in this case a skeptical District Court concluded that Chamberlain’s DMCA claims for trafficking in an anticircumvention device failed. In particular, the court concluded that the plaintiff had failed to show lack of authorization to access the security code, because the purchasers had an expectation or implied license to use the garage opening device they purchased with a second compatible remote control. Thus, the competitor Skylink could not be supplying a device for unauthorized access. This holding of course left open the possibility that such a license might be revoked by a restrictive express license, such as a mass-market “shrink-wrap” contract, but such a contract claim was not at issue in the suit.

---

<sup>139</sup> *Id.*

And surprisingly, on appeal, the Federal Circuit not only upheld the District Court's result, but expanded and amplified the holding in an opinion with potentially broad applicability to DMCA claims targeted at non-infringing interoperable devices.<sup>140</sup> The appellate opinion focused on the lack of any relationship between the access enabled by the Skylink device, and a copyrighted work. The court factually distinguished such cases, such as *Remierdes*, and the trial court opinion in *Lexmark*, as involving an allegation of copyright infringement. Chamberlain, in contrast, had alleged no infringement of its underlying software. Indeed, the Federal Circuit agreed with the trial court that authorization for use of the door opening software was implied in the purchase of the Chamberlain product, precluding a claim of unauthorized exercise of an exclusive right of the copyright holder.

The Federal Circuit also rejected language from previous decisions, such as that in *Remierdes*, suggesting that the DMCA anticircumvention provisions should be read as creating a new right of access to protected works.<sup>141</sup> The court was particularly exercised to reject any proposal that the anti-circumvention provisions create a new form of property right. According to the Federal Circuit opinion, Congress intended the DMCA anti-circumvention provisions to secure the technical protection of copyrighted works, and not as a new set of legal privileges in their own right. Thus, the opinion treats the anticircumvention provisions as prohibiting only forms of access that bear a reasonable relationship to the rights granted by the copyright act.<sup>142</sup>

Close on the heels of the *Chamberlain* decision, the 7<sup>th</sup> Circuit Court of Appeals repudiated the determination of the trial court in the *Lexmark* case. Like the appellate

---

<sup>140</sup> Chamberlain Group, Inc. v. Skylink Tech., Inc. 381 F.3d 1178 (Fed. Cir. 2004).

<sup>141</sup> *Id* at 1199.

opinion in *Chamberlain*, the appellate opinion in *Lexmark* rather clearly displays the courts' concern that such DMCA claims had nothing to do with the pirating of music or other copyrighted content; but rather, constituted a fairly naked attempt to suppress competition in the market for printer ink cartridges. The appellate opinion sharply reversed the trial court's reasoning, holding that the Lexmark codes utilized by the Static Control chips did not control "access" to the printer software; the software code was not encrypted or otherwise protected by technical measures.<sup>143</sup> By purchasing a printer, the court reasoned, an owner could access, read, and alter the software at will. Neither did the court accept that the codes controlled access to the printer software in the sense of controlling its use. Additionally, the 7<sup>th</sup> Circuit appeared sympathetic to a broader interpretation of the DMCA reverse engineering provision, holding that the Static Control chip contained software that appeared to constitute "independently created" programs for which interoperability was needed; consequently, the reverse engineering exception might apply to Static Control's activities.

When taken together, these appellate opinions suggest that the judicial system is becoming aware of the potential for abuse of the DMCA, and is searching for limitations to the broad approval articulated in earlier decisions. It remains unclear how robust these particular results will be. The *Chamberlain* decision relies heavily on the lack of a copyright claim to distinguish the case from previous cases applying the anti-circumvention provisions. In one sense, this distinction moves in the correct direction, tying the DMCA back to its original purpose as a deterrent against copyright piracy. But as a practical matter, the inclusion of a copyright claim seems all that is necessary to

---

<sup>142</sup> *Id.* at 1202-03.

<sup>143</sup> *Lexmark Inc. v. Static Control Components Inc.*, 2004 U.S. App. LEXIS 22250 (6<sup>th</sup> Cir. Oct. 26, 2004).

place future cases into the same category as the claims in *Remierdes* or *Streambox*. Incorporating an allegations of copyright infringement into an anticircumvention presents a rather low threshold for DMCA claims; because technical protections will nearly always include some software component, inclusion of a copyright claim to accompany circumvention claims will be routine, even if no digital content is truly at risk.

Additionally, the *Chamberlain* appellate opinion, as the trial court opinion, leaves open the use of mass-market licenses to prevent reverse engineering or interoperation of technically protected devices with unauthorized devices. Although the *Chamberlain* court declined to reach the question of whether circumvention could be prohibited by mass-market contract,<sup>144</sup> Federal Circuit precedent might be read to allow such a prohibition.<sup>145</sup> The *Lexmark* decision, too, relies heavily on access privileges inferred from purchase of a device, when such privileges could in theory be restricted by “shrink-wrap” boilerplate. If such uses of “shrink-wrap” are permissible, then boilerplate licenses might be employed to negate whatever limits have placed on strategic overreaching by means of the DMCA anticircumvention provisions.

## **VI. Competitive Antidotes**

I have argued that, like any other interoperable computer technology, DRM will tend towards a single standard, and simultaneously towards whatever concerns over monopolization or restraint of trade that come with such network effects. Additionally,

---

<sup>144</sup> *Id.* at n. 17.

the secure computing features of DRM will tend to resist the market forces that would naturally tend to ameliorate such concerns. But it is the approach to anti-circumvention law adopted in decisions such as *Reimerdes*, *Blizzard*, and the trial court *Lexmark* opinion that most greatly heightens the danger of such anti-competitive effects. The facts of these cases illustrate the kind of anti-competitive uses to which anti-circumvention claims might be put, and the reasoning in such opinions essentially blesses the most pernicious application of the DMCA provisions.

The development of technical standards in general has been recognized as raising concerns under both Section 1 of the Sherman Anti-trust Act, which prohibits conspiracies to restrain trade<sup>146</sup>, and under Section 2 of the Act, prohibiting monopolization or attempted monopolization.<sup>147</sup> Under Section 1, there may be concern that standard-setting organizations will act as cartels to exclude new entrants; under Section 2, there may be concern that the owner of a proprietary standard will exploit network effects to dominate a particular market. On rare occasions, courts have also recognized certain design choices as technological attempts to “tie” together interoperable products, effectively excluding consumer adoption of products produced by competitors because of technological incompatibility.<sup>148</sup> Such “predatory design” situations might be penalized as a form of anti-trust violation if anti-competitive intent, rather than technological benefit prompted the design.<sup>149</sup> This kind of anti-trust claim has

---

<sup>145</sup> See *Bowers v. Baystate*, 320 F.3d 1317 (Fed. Cir. 2003).

<sup>146</sup> 15 U.S.C. § 1.

<sup>147</sup> 15 U.S.C. § 2.

<sup>148</sup> See 1 H. HOVENKAMP, ET AL. *supra* note \_\_ at § 12.3c.

<sup>149</sup> *Response of Carolina, Inc. v. Leasco Response, Inc.*, 537 F.2d 1307, 1330 (5th Cir. 1976).

been controversial<sup>150</sup>, and in its present form could be difficult to employ if incompatibility is claimed for the purpose of “secure computing.”

The difficulty of formulating an anti-trust claim under either section of the Sherman Act stems from the need for a “rule of reason” balancing approach, comparing benefits to detriments.<sup>151</sup> In general, standard-setting, whether for DRM or other forms of interoperation, will create a variety of pro-competitive benefits: the creation of compatible consumer products, enhancement of positive network effects, avoidance of incompatible products that could leave consumers “stranded” when other standards become dominant. Typically, many of these benefits can be captured by firms that are not part of the standard-setting process. Indeed, some commentators on standards-setting organizations have raised the concern that follow-on firms might “free ride” on the standards-setting process, avoiding the costs of standard-setting by not participating in the process, but reaping the rewards of compatibility by following the standard once it is in place.<sup>152</sup>

Whether such free-riding is in itself desirable or not, it mitigates concern over anti-competitive exclusion; once a standard is established, firms can typically at essentially zero cost adopt the established standard and incorporate it into their products so that markets and consumers will benefit. But the ability to adopt a standard assumes accessibility to or familiarity with that standard. Analyses of standards-setting that rely upon open adoption of standards likewise assume that firms in the marketplace will be

---

<sup>150</sup> See Joseph Gregory Sidak, *Debunking Predatory Innovation*, 83 COLUM. L. REV. 1121 (1983) (arguing against recognition of claims for anticompetitive design); *but see also* Janusz A. Ordover, Alan O. Sykes & Robert O. Willig, *Predatory Systems Rivalry: A Reply*, 83 COLUM. L. REV. 1150 (1983) (refuting Sidak critique of predatory design claims).

<sup>151</sup> See Michael A. Carrier, *Why Antitrust Should Defer to the Intellectual Property Rules of Standard-Setting Organizations: A Commentary on Teece & Sherry*, 87 MINN. L. REV. 2019, 2032 (2003).

able to comprehend and mimic the standard through examination or reverse engineering of the products incorporating the standard. Under such conditions, the anti-competitive effects of network “lock-in” will be at least somewhat ameliorated by the threat of new entry, so long as new entrants can adopt or adapt the standard.

Such standards adoption may be frustrated if the standard is protected by intellectual property rights so that reverse engineering and adoption of the standard may constitute intellectual property infringement.<sup>153</sup> Patents pose a particular problem in this context, as patent law contains no reverse engineering provision, and indeed, hardly any exemptions from infringement at all.<sup>154</sup> Copyright has on occasion been interposed to prevent reverse engineering of software products<sup>155</sup>, but presents less of a problem than patents, due to a line of cases holding that copying in the course of reverse engineering may constitute fair use.<sup>156</sup> Either form of exclusive right could in theory be employed to anti-competitive effect in violation of the antitrust law, but the general trend, especially for patents, has increasingly been one of deference to the right holder, making the limit of impermissible exclusion increasingly remote.

As a consequence, commentators have given considerable attention to the problem of standards promulgation when that standard is covered by a patent, including discussion of the proper role of antitrust and misuse law in deterring the anti-competitive

---

<sup>152</sup> See Lemley, *supra* note \_\_\_ at 1053; Teece & Sherry, *supra* note \_\_\_ at 1980; Carrier, *supra* note \_\_\_ at 2032-33 (2003).

<sup>153</sup> See Mark R. Patterson, Inventions, Industry Standards, and Intellectual Property 17 BERKELEY TECH. L.J. (2002).

<sup>154</sup> See Maureen O'Rourke, *Toward a Doctrine of Fair Use in Patent Law*, 100 COLUM. L. REV. 1177 (2000).

<sup>155</sup> See Julie E. Cohen, *Reverse Engineering and the Rise of Electronic Vigilantism: Intellectual Property Implications of “Lock-Out” Programs*, 68 SO. CAL. L. REV. 1091 (1995).

<sup>156</sup> See O'Rourke, *supra* note \_\_\_; Julie E. Cohen & Mark A. Lemley, *Patent Scope and Innovation in the Software Industry*, 89 CAL.L.REV. 1 (2001).

effects of proprietary standards.<sup>157</sup> But the problems identified in this regard may be far more common, or greatly exacerbated, when the standard involves DRM. In order to remain secure, such devices will typically be designed to resist casual examination and interoperation with non-trusted devices. Reverse engineering of such devices will require circumvention of their security measures. Thus, detailed examination of DRM standards, including decryption and reverse engineering, will likely run afoul of the DMCA anti-circumvention provisions, creating a legal deterrent to competitive or interoperable products.

As interpreted in *Remeirdes* and similar cases, the anti-circumvention provisions may therefore play the role that patents sometimes play in suppressing device interoperation.<sup>158</sup> When interpreted as a type of exclusory right, these provisions force firms that wish to adopt the DRM standard to ask for permission, for a license; if the license is denied, attempting self-help violates the DRM owner's anti-circumvention right. The fair use exemption for reverse engineering would not apply, since under this view circumvention is prohibited for both fair use and foul. Neither is the DMCA reverse engineering exception likely to avail; by its own terms it applies only to software interoperation, and the analysis in cases such as *Blizzard* limits the exception further to "independent" products that are not substitutes for the work examined.

The result of this approach would allow DRM developers to leverage technical standards into aftermarket monopolies covering a wide range of interoperable devices and substitute – precisely the pattern of exclusion seen in the DMCA cases up until

---

<sup>157</sup> See Michael A. Carrier, *Unravelling the Patent-Antitrust Paradox*, 150 U. PA. L. REV. 761 (2002); Janice Mueller, *Patent Misuse Through Capture of Industry Standards*, 17 BERKELEY TECH L.J. 623 (2002); Patterson, *supra* note \_\_\_\_; Mark R. Patterson, *When is Property Intellectual? The Leveraging Problem*, 73 S. CAL. L. REV. 1133 (2000);

*Chamberlain*. The *Chamberlain* and *Lexmark* opinions radically change the trend begun in *Remierdes* by reinterpreting the statute to avoid the strategic behavior that had begun to emerge from . The Federal Circuit's language rejected the proposition that the anti-circumvention provisions create a new form of property right, effectively transforming the anti-circumvention provisions into a sort of "super contributory" infringement. Analytically, this ties anti-circumvention claims to back to copyright, reintroducing into the anti-circumvention provisions the standards-based determinations found in the copyright act – if for example, the use of the protected content was fair, no anti-circumvention claim would lie.

At the same time, the *Chamberlain* and appellate *Lexmark* opinions also recognize that the development of DRM is not exempt from the prohibitions of anti-trust law and doctrines of misuse. Both opinions leave open the possibility of contractual access prohibitions, which in combination with the anti-circumvention prohibitions could cross the line into anti-competitive conduct. The *Chamberlain* approach rejects the formulation of anti-circumvention rights as separate from copyright, but were the *Remeirdes* approach to prevail, and the anti-circumvention provisions considered to constitute a separate property right, the opinion recognizes that it would still be constrained by anti-trust law. Similarly, the opinion seems to caution against permitting copyright owners to use combinations of technical protections and contract to prohibit certain uses, such as fair uses of a copyrighted work, when the public has "an inherent legal right" to such uses.<sup>159</sup> Anti-trust seems to be at least one suggested limitation to overreaching under either a contractual or property-based theory, as the anti-trust claims

---

<sup>158</sup> See Cohen, *supra*, note \_\_\_ at 1190 (1995).

<sup>159</sup> *Id.* at 1202

that have been at issue in previous standards-setting, such as claims of tying or concerted refusal to deal, may for the reasons I have indicated above be heightened in the DRM milieu.

The *Chamberlain* opinion also suggests a role for the related but separate doctrine of misuse. I have similarly argued that misuse might be pressed into service to curtail overreaching under the DMCA.<sup>160</sup> This employment of misuse seems highly appropriate if anti-circumvention is viewed as a collection of rights separate from copyright in the underlying technically protected work – a position vehemently rejected by the *Chamberlain* opinion.<sup>161</sup> But misuse remains an appropriate antidote for overreaching even if the anti-circumvention provisions are viewed as a form of super-contributory infringement. The doctrine of misuse for many years acted as a foil or counterbalance to expansive contributory infringement in patent law, and appears to be taking on much the same role in copyright.<sup>162</sup> Misuse might well undertake a similar function regarding a new “super” contributory infringement right under the DMCA.

## **Conclusion**

In this paper I have examined certain social costs of deploying digital rights management or “DRM” systems to protect copyrighted content, although I have limited my examination to “hard” systems directed to active control or prohibition of content usage. I have not considered “soft” DRM measures, such as steganography or “watermarking” that might enhance detection and enforcement of existing legal

---

<sup>160</sup> See Dan L. Burk, *Anti-Circumvention Misuse*, 50 UCLA L. REV. 1095 (2003).

<sup>161</sup> 381 F.3d at 1199.

prohibitions, and so indirectly deter certain user behaviors. “Hard” technologies have been the subject of intense interest by content producers, as these technologies hold the promise of self-enforcement.

But the calculus of costs and benefits at for such technical self-help is highly complex, and the prospect for successful “self-help” via such measures is uncertain. The nature of this technology tends away from the embodiment of legal standards, but toward the formulation of uniform technical standards. The first trend implicates heightened costs from ex ante design of behavioral constraints; it seems unlikely that content producers possess sufficient information about the uses of content in order to make a correct decision regarding the design of DRM restrictions. Some consideration for the value of overly restricted access may be reflected in lower prices for DRM restricted products, however, much of the value of unrestricted access may be unpredictable or diffuse.

The second trend suggests strategic reasons as to why content developers may have improper or insufficient incentives for taking into account consumer preferences or value. DRM will tend not only toward a technical standard, but toward a technical standard that may be uniquely susceptible to strategic manipulation. This susceptibility appears to have been reinforced by the passage of anti-circumvention legislation that in fact lends itself to an anti-reverse engineering interpretation. Recent appellate cases involving the anti-circumvention provisions suggest that courts are willing to re-interpret the statute in order to deter the most egregious behavior fostered by such an interpretation. But it is unclear how robust this re-interpretation might be, inviting a re-

---

<sup>162</sup> See Burk, *supra* note \_\_\_\_.

Draft of 1/31/2005. Please do not quote or cite without author's permission.

consideration of competition doctrines such as predatory design and misuse in the context of DRM standards.