IP central
Academic Advisory Council

THE PROGRESS & FREEDOM FOUNDATION'S
Center for the Study of Digital Property

DEFUSING DRM

The introduction of digital rights management technology is not the watershed event some deem it to be.

Academic Advisory Council
Bulletin 1.1

by Doug Lichtman*

Ten years ago, a meaningful discussion of copyright law could focus almost exclusively on the federal copyright statute and related case law. At that time, the primary powers wielded by copyright holders were rights granted explicitly by the statute, such as the exclusive rights to authorize duplication, distribution, adaptation, and performance. The primary constraints on copyright power, meanwhile, were similarly found in statutory text. Section 107, for example, forbid copyright holders from enforcing their rights against "fair use" infringements like parody and scholarship. Section 102 made clear that copyright protection could not be used to restrict access to ideas, concepts, and principles. In short, the relationships between and among authors, readers, viewers, and listeners were dictated by explicit government rules.

Today, by contrast, technology takes center stage. For instance, in the iTunes music store, it is not copyright law, but encryption algorithms that restrict consumers from playing purchased tunes on portable devices other than the officially-sanctioned iPod. Likewise, on music CDs distributed by Sony BMG, it is not the threat of litigation, but computer software that discourages purchasers from copying tracks for friends or personal use. These are just two among many examples of what has come to be known as "digital rights management" (DRM) technology. And, with DRM now increasingly mainstream, it is finally time to ask publicly a question that academics, technologists, and some policy-makers have been quietly discussing for some time: How should copyright law respond?[1]

---

*Doug Lichtman is a professor of law at the University of Chicago. The views expressed are the author's own. Comments on this piece may be sent to advisory@ipcentral.info. Comments and responses may be posted on the IPcentral Weblog. This piece can be cited as Doug Lichtman, Defusing DRM, IP Academic Advisory Council Bulletin 1.1 (February, 2006)

[1] Three early and thoughtful contributions on this question were LAWRENCE LESSIG, CODE AND OTHER LAWS OF CYBERSPACE (1999); Joel Reidenberg, *Lex Informatica: The Formulation of Information Policy Rules Through Technology*, 76 TEX. L. REV. 553 (1998); and Tom Bell, *Fair Use vs. Fared Use: The Impact of Automated Rights Management on Copyright's Fair Use Doctrine*, 76 N. CAROLINA L. REV. 557 (1998).

BIG CHANGE, OR SMALL?

Start with a related question: How significant a change will the introduction of DRM be in practice? Reasonable minds might disagree, and in part the jury is still out, but my own view is that for several reasons the change will not be particularly severe. First and most obviously, consumers seem to disfavor protected content, and thus there is significant financial pressure not to adopt these technologies. When I purchase a DVD, for instance, I want to be able to watch it in my home DVD player and I also want to be able to drop it onto my video iPod and watch it on the train. The motion picture studios can use DRM to stop the latter activity—just as they could, in theory, double the price of the movie or charge me extra for deleted scenes—but the binding constraint in all of these choices is the law of supply and demand, not some limitation based on what technologies are or are not available.

Second, hackers have thus far been remarkably effective at defeating DRM systems. One of Sony BMG's early copy protection technologies, for example, was outsmarted by a hacker who realized that the protection software could be blocked by a strategically placed piece of tape. Another Sony system gave way when a hacker thought to press the SHIFT key while loading protected music. This history renders implausible the fear that every scrap of content will someday be trapped behind lock and key. Put differently, there has been and always will be an arms race between those who want to restrict access and those who want to set content free, and it seems overly optimistic to imagine that either side will ever achieve a stable and decisive victory over the other.

Third, even at the theoretical extreme, DRM can only be so controlling. It is hard to imagine how any technology could stop a person from hearing a song and then later humming it in the shower or creating a humorous parody. Indeed, the Achilles heel in every system designed to control content is that at some point customers must be able to read, hear, or otherwise experience the purchased information. Whenever that happens, the information is necessarily exposed and hence vulnerable to use and access that the relevant author might not like.

Fourth, and a point often missed in discussions of DRM, content owners do not necessarily want airtight control over their work, and so there is no reason to expect that they will use extreme forms of DRM even if extreme forms were feasible. Magazine publishers, for example, likely benefit from the fact that consumers share magazines, passing a given issue from one friend or family member to another. Sharing in this manner is a less expensive way to distribute magazines than is the next-best alternative of printing, packaging, and shipping another copy. Thus, as long as a publisher can pick up sufficient extra revenue from the sharing—say, charging a higher price for the original magazine or

generating more ad revenue thanks to higher readership numbers[2]—the publisher has little incentive to thwart the practice. Sharing makes everyone better off, with both publishers and consumers benefiting from the savings made possible through the use of a cheaper distribution channel.[3]

DRM IN CONTEXT

If I am right in all this—if DRM will be potentially strong but not Orwellian—the next step in the analysis is to recognize that to some degree every area of legal endeavor follows this same basic pattern. There is a formal set of rules enforced by judges, administrative officials, and the like, and there is a weak but effective overlapping capacity through which private actors can take matters into their own hands.[4] This is an intuitive point in a field like criminal law, where bad actors are deterred in part by official sanctions like the threat of jail time and the prospect of police intervention, and in part by the knowledge that homeowners have guns, security systems, and other private means by which to defend their property. But it is in fact true almost everywhere. Entrepreneurs, for example, use the formal mechanisms of patent and trade secret law to protect proprietary information. But they also use private mechanisms: dividing sensitive information across employees such that no single employee ever knows enough to betray the firm completely; creating long-term stock programs that serve to discourage employees from defecting to rival firms; hiring friends and family members for sensitive positions rather than more qualified candidates on the assumption that personal ties breed loyalty. Similarly, in the realm of privacy law, various statutes and doctrines restrict the disclosure of personal information, but individuals supplement those formal protections by drawing their shades, speaking white lies, and storing their diaries behind lock and key.

---

[2] For the details, see Stanley M. Besen & Sheila N. Kirby, *Private Copying, Appropriability, and Optimal Copyright Royalties*, 32 J.L. & ECON. 255 (1989); Yannis Bakos, Erik Brynjolfsson & Douglas Lichtman, *Shared Information Goods*, 42 J.L. & ECON. 117 (1999).

[3] The literature on digital rights management typically blurs an important distinction relevant to this question of whether content owners want absolute control: the distinction between perfect price discrimination—where a seller knows exactly how much a given consumer values a given content product and can price accordingly—and control of the sort I discuss in the text, where a seller at best might know how often a consumer listens to a given song, and when, and from where. To be sure, the latter is a proxy for the former, but it is not a substitute. Knowing how often you listen to a given music CD might hint at how much you value it, but there is slippage between these two types of information. Content holders admittedly would love to be able to practice perfect price discrimination. But that does not imply that they also will use technology to exercise complete control. As the magazine example makes clear, control might not be in their interest, even though price discrimination clearly is.

[4] This link between private and public mechanisms is one of the central themes in Lawrence Lessig's influential book, cited above in note 1. This same theme has been fruitfully explored in a variety of other settings as well. For example, Neal Katyal has written several informative articles applying this intuition to criminal law. *See, e.g., Architecture as Crime Control*, 111 YALE L.J. 1039 (2002); *Community Self-Help*, 1 J. L. ECON. & POLICY 33 (2005).

At a certain level of generality, then, every area of law is properly characterized as an interaction between public remedies and private self-help alternatives. Copyright law has long been an exception to this rule, in that authors have not previously had any effective self-help remedy by which to protect their work after publication. DRM simply brings copyright law into the fold.

This is of course not to imply that all DRM should be embraced. Some self-help technologies are so powerful, or so potentially harmful, that they are and should be substantially regulated. The privilege of self-defense is an example here. A crime victim cannot invoke the privilege to excuse just any act of violent self-help—remember Bernard Goetz? The privilege instead excuses violence only in a narrow set of circumstances, for example instances where the victim has exhausted all reasonably safe, alternative means of mitigating some imminent physical threat.[5] That said, experience throughout the law suggests that, as a general rule, banning the use of self-help mechanisms is not the answer. Quite the opposite, legal rules typically interact with self-help remedies in a much more complicated and mutually reinforcing manner.

TRADE SECRET LAW. Consider trade secret law.[6] Under the Uniform Trade Secrets Act, trade secret protection is extended only if three conditions are met: the information is secret and derives economic value from that secrecy; the information was taken by improper means like trespass or breach of contract; and—this is the important one for current purposes—at the time of the improper taking, the information was itself subject to reasonable precautions to maintain its secrecy.[7] Notice what this means: In trade secret law, self-help is a required precondition to formal legal protection. The obvious reason is that self-help in this setting is typically more cost-effective than any formal legal alternative. Why bring in the lawyers when a simple fence will do? A more subtle explanation is that, where legal intervention is necessary, self-help lowers evidentiary costs by providing helpful circumstantial evidence that a given trade secret was in fact taken unlawfully. Imagine how much more difficult it would be to evaluate allegations of trade secret misappropriation if secrets were routinely kept in glass buildings.[8] Yet a third explanation is that self-help in this setting serves to distinguish normal business information from that special subset of information that warrants protection. The idea is to keep the scope of trade secret protection

---

[5] RESTATEMENT (SECOND) OF TORTS § 63(1).

[6] Two other helpful and sometimes contradictory accounts of the economics of trade secret protection are David D. Friedman et al., *Some Economics of Trade Secret Law*, 5 J. ECON. PERSP. 61 (1991); and Robert G. Bone, *A New Look at Trade Secret Law: Doctrine in Search of Justification*, 86 CAL. L. REV. 241, 262-72 (1998).

[7] UNIF. TRADE SECRETS ACT § 1 (defining the terms "trade secret" and "improper means").

[8] For a parallel argument applied to copyright law—again the core insight being that many legal doctrines can and should exclude from protection cases that are prone to evidentiary complexity—see Douglas Lichtman, *Copyright as a Rule of Evidence*, 52 DUKE L.J. 683 (2003).

in check by only protecting information in cases where the relevant trade secret holder signaled, up front, that the information at issue was valuable.[9]

My comments thus far emphasize self-help as a tool that makes the protection of trade secrets more efficient. Interestingly, self-help is also an important means by which certain secrets leak. Unpacking that a bit: under current law, a competitor is permitted to purchase a rival's product, smash it to pieces on the ground, and then study those remnants to learn whatever secrets they might reveal. This form of self-help is typically referred to as reverse engineering, and—unlike alternative approaches like bribing a rival's employees or sneaking onto a rival's premises at night—reverse engineering is a form of secret-stealing that trade secret law deems perfectly permissible.[10] Reverse engineering does create some social waste. The threat of reverse engineering causes secret-holders to introduce unnecessary complexity into their products by (say) favoring designs where the critical step is accomplished by a hard-to-crack software process rather than a cheaper but more transparent hardware equivalent. Nevertheless, trade secret law allows reverse engineering on the theory that the additional flow of information more than compensates for any resulting waste. Moreover, reverse engineering is an attractive means by which to encourage this desirable information leakage because, unlike bribery and trespass, reverse engineering is unlikely to directly disrupt a trade secret holder's business operations or lead to physical confrontation.[11]

PRIVACY LAW. Turn now to privacy law. If trade secret law is rightly understood as a body of law that encourages self-help from secret-holders and rivals alike, privacy law represents something of the opposite approach: privacy protections are primarily designed to displace plausible self-help alternatives. Put differently, modern privacy law is at first blush puzzling in that it in various ways

---

[9] *See* ROBERT P. MERGES ET AL., INTELLECTUAL PROPERTY IN THE NEW TECHNOLOGICAL AGE 50 (3d ed. 2003) ("one might treat the requirement of reasonable precautions as serving a gate-keeper function to weed out frivolous trade secret claims by requiring evidence of investment by the plaintiff in protecting the secret"); Edmund W. Kitch, *The Law and Economics of Rights in Valuable Information*, 9 J. LEGAL STUD. 683 (1980) (precautions serve to distinguish secrets from everyday unprotected information).

[10] Reverse engineering can take a variety of forms, such as testing the properties of a competitor's product or decompiling a competitor's computer code. See UNIF. TRADE SECRETS ACT §1 cmt. 1 (amended 1985) (identifying as a proper means of discovery the act of taking a "known product and working backward to find the method by which it was developed").

[11] Although I believe that reverse engineering should often be permissible, I should point out that I am skeptical of the privilege in certain applications. For example, some types of reverse engineering are so cheap that they threaten to fully undermine the incentive to engage in innovative activity in the first place. In those circumstances, it might be attractive to allow for some form of prohibition against the cheap copying technique. *See* Douglas Gary Lichtman, *The Economics of Innovation: Protecting Unpatentable Goods*, 81 MINN. L. REV. 693 (1997). Similarly, reverse engineering sometimes undermines beneficial coordination within an industry. An example here is the market for home video-game consoles, where reverse engineering makes it difficult for console makers to coordinate the development of complementary goods like software and hardware peripherals. *See* Douglas Lichtman, *Property Rights in Emerging Platform Technologies*, 29 J. LEGAL STUD. 615 (2000).

restricts the disclosure of private facts related to personal finances, sexual orientation, medical conditions, and the like, even in instances where public revelation might serve social interests. Imagine, for example, if information about sexual promiscuity and sexual orientation could be acquired and disseminated without fear of legal liability. The former would do much to protect unsuspecting partners from the dangers of STDs, while the latter might significantly de-stigmatize what are still today controversial closet preferences. Yet the law protects these facts, and it arguably does so because, in the absence of protective legal rules, individuals would protect their privacy anyway, and would do so in ways that are more wasteful still. Patients would withhold vital information about their sexual history from doctors; adults discussing personal matters would speak in tongues; and lovers interrupted in the privacy of their homes would on occasion resort to violence. In sharp contrast to trade secret law, then, with respect to privacy the formal protections offered under the law might be best explained as rights meant to obviate what would otherwise be effective but costly self-help measures.[12]

Avoiding the costs associated with self-help is actually a common justification for formal legal intervention. Major League Baseball's Chicago Cubs, for instance, were recently involved in a dispute with several firms that own rooftop properties overlooking the Cubs' home stadium, Wrigley Field.[13] At issue were what are in essence unauthorized stadium skyboxes—complete with plush seats, fancy catering, and full service bars—built on those nearby rooftops and to which tickets are sold to watch Cubs baseball. The Cubs understandably thought this practice unfair; rooftop seats compete with stadium seats and yet the rooftop owners were contributing nothing toward team salaries or stadium upkeep. Thus, the Cubs engaged in a little self-help: the team installed a large canvas windscreen that just so happened to block the view from several rooftop properties. The rooftop owners in response made plans to raise their rooftop seats higher; and, by the time a court began hearing the merits of the dispute,

[12] Privacy law does permit disclosure in instances where the revelation of a private fact seems to serve an immediate and important social interest. A psychiatrist, for example, can and indeed must break the doctor/patient privilege if he learns that his patient is about to commit a violent crime. *See* Tarasoff v. Regents of the University of California, 551 P.2d 334 (Cal. 1976). Medical professionals have similarly been held liable for failing to warn a patient's spouse that the patient was suffering from a dangerous and communicable disease. *See* Bradshaw v. Daniel, 854 S.W.2d 865 (Tenn. 1993). Recognizing exceptions, however, is a far cry from refusing to protect the information outright. With respect to STDs, for instance, it is implausible to think that a knowledgeable party will be able to identify in advance every vulnerable sexual partner and quietly warn that partner of the medical risks ahead. The exception in favor of such disclosures thus accomplishes little. The partner would be much more richly protected in a world where information about sexual promiscuity were freely available. Privacy law does not take that step, however, because self-help makes that outcome unattainable.

[13] *See* Jodi Wilgoren, *Cubs Sue Neighborhood Bars on Rooftop Use*, N. Y. TIMES, Dec. 18, 2002, at D4. I was directly involved in this particular dispute—I advised the Cubs on questions related to copyright preemption—so I should make expressly clear that the brief discussion here represents my own views and draws only on information publicly available.

rumor had it that the Cubs were planning to construct a giant balloon that would have randomly obscured even elevated rooftop views. Stopping this "arms race" was one of the core reasons that a court ultimately intervened. Self-help here was in each party's short-term private interest but it was in the aggregate wasting resources and worsening the baseball experience both within the stadium and above it.

THE FIRST AMENDMENT. A final example of the interaction between formal legal rules and private self-help alternatives can be drawn from First Amendment jurisprudence, where, in most instances, the existence of a cost-effective self-help remedy is taken to be an argument against using government regulation as a means to accomplish a similar end.[14] When the city of Los Angeles arrested a war protestor whose jacket bore the now-infamous "Fuck the Draft" inscription, for example, the Supreme Court held the relevant ordinance unconstitutional. Offended viewers, the court explained, have a sufficient self-help remedy in the form of simply averting their eyes.[15] Similarly, in a long line of cases involving speakers caught advocating crime, sabotage, and other forms of violence as a means of achieving political or economic reform, the Court (albeit after a false start or two[16]) again struck down government restrictions, emphasizing that, where there is "time to expose through discussion the falsehood and fallacies, to avert the evil by the processes of education, the remedy to be applied is more speech, not enforced silence."[17]

Self-help in these and other First Amendment settings is favored because of two compelling charms. First, self-help makes possible diverse, individuated judgments, increasing the flow of information by not only allowing willing speakers to reach willing listeners but also empowering unwilling listeners to opt out of unwanted communication at low cost. Second, and perhaps more central, self-help reduces the government's overall role in regulating speech, an important outcome given that the First Amendment is in general suspicious of

---

[14] Excellent discussions on the general topic of how self-help opportunities affect First Amendment jurisprudence include Douglas Ivor Brandon et al., *Self-Help: Extrajudicial Rights, Privileges and Remedies in Contemporary American Society*, 37 VAND. L. REV. 845, 855-58 (1984); Tom W. Bell, *Free Speech, Strict Scrutiny, and Self-Help: How Technology Upgrades Constitutional Jurisprudence*, 87 MINN. L. REV. 743 (2003).

[15] *See* Cohen v. California, 403 U.S. 15, 21 (1971) ("Those in the Los Angeles courthouse could effectively avoid further bombardment of their sensibilities simply by averting their eyes.").

[16] *See, e.g.*, Abrams v. United States, 250 U.S. 616 (1919).

[17] Whitney v. California, 274 U.S. 357, 377 (1927) (Brandeis, J., concurring). The quote ought not be taken too literally. For example, surely the touchstone is not "time"; in many instances, there will be no meaningful future opportunity to reach the tainted audience no matter how much time might pass, and in such cases additional speech would be an empty remedy. That caveat aside, the Court often invokes this idea of speech chasing speech. *See, e.g.*, Gertz v. Welch, 418 U.S. 323, 344 (1974) ("The first remedy of any victim of defamation is self-help—using available opportunities to contradict the lie or correct the error and thereby to minimize its adverse impact on reputation.").

government regulation for fear that some manipulative government official will use a seemingly innocuous regulation to advance a particular viewpoint.

The above examples are instances where the existence of a plausible self-help remedy posed a challenge to the government's claim that some formal speech restriction was required. But in First Amendment jurisprudence the opposite argument also plays a prominent role: where a "captive audience" has no effective self-help mechanism by which to avoid exposure to a given communication, that absence of a plausible self-help mechanism is taken to be an argument in favor of direct government regulation.[18] The point was famously made in *Lehman v. Shaker Heights*. The city of Shaker Heights, Ohio, had decided to allow advertisements to be displayed inside its public transit system, and four Justices emphasized audience captivity as an important factor in justifying a companion restriction on the types of advertisements allowed.[19] A year later, in *Erznoznik v. Jacksonville*, the Court considered a local ordinance designed to stop drive-in movie theaters from displaying potentially offensive visuals in instances where the images would be visible from the public streets. Again, six Justices stressed self-help, endorsing the view that the government can selectively "shield the public" in cases where "the degree of captivity makes it impractical for the unwilling viewer or auditor to avoid exposure."[20]

LESSONS LEARNED

Applying all this back to copyright law, there are obviously dozens of worthwhile analogies to draw. Maybe DRM designed to combat piracy ought to be treated by copyright law the same way that trade secret law treats private attempts to maintain secrecy. In both settings, after all, it seems plausible to expect that self-help is cheaper and more effective than traditional legal enforcement. At the same time, in both settings it is valuable to allow some information leakage—and thus the Digital Millennium Copyright Act likely goes too far when it in essence forbids the distribution of any technology that might be used to crack DRM systems.[21]

---

[18] On this theory, the less a listener is able to defend himself from an unwanted message, the greater the government's interest in either facilitating self-help, or directly regulating the unwelcome speaker. To say that an audience is "captive" is thus to say that the costs of engaging in self-help are particularly high. *See* Bell, cited in note 14, at 752 ("An audience qualifies as 'captive' only if it lacks attractive self-help remedies for countering offensive speech."). For a general introduction to the captive audience doctrine, see Geoffrey R. Stone, *Fora Americana: Speech in Public Places*, 1974 SUP. CT. REV. 233. For criticisms, see Doug Lichtman, *How the Law Responds to Self-Help*, 1 J. L. ECON & POL'Y 215, 222-25 (2005).

[19] Lehman v. Shaker Heights, 418 U.S. 298, 302-04 (1974).

[20] Erznoznik v. Jacksonville, 422 U.S. 205, 209 (1975). The six then announced that in this particular situation the necessary degree of captivity was not realized because drivers could simply look away. *Id*. at 212.

[21] *See* 17 U.S.C. § 1201(a)(2) & (b)(1).

With respect to DRM in the form adopted by iTunes, meanwhile, maybe copyright law should adopt nuanced rules like those that today limit the scope of the privilege of self-defense. The commonality here is that in both instances self-help ought not be allowed to become too common. Frequent self-defense would give rise to a vigilante state; widespread iTunes-style restrictions would reduce hardware competition by in essence making it impossible to enter the hardware market without simultaneously entering the relevant content business as well.[22]

For now, however, my goal is neither to pursue these analogies nor to catalog in full form the many ways that legal rules encourage, harness, deter and sometimes defer to self-help.[23] My message is instead more fundamental. Legal rules in every area of human interaction are implemented through a combination of powerful public mechanisms and weaker but less costly private ones. With the advent of DRM, copyright law is today no different. The task now is not to legislate DRM out of existence, but instead to follow the model adopted in every other arena: calibrate copyright law such that it harnesses the very real advantages of technological enforcement while at the same time keeping an appropriately wary eye on what might turn out to be overly aggressive uses.

[22] Readers familiar with antitrust law will recognize the concern here as a concern about bundling—in particular bundling that might raise a non-trivial barrier to entry. See generally HERBERT HOVENKAMP, FEDERAL ANTITRUST POLICY: THE LAW OF COMPETITION AND ITS PRACTICE 372-375 (1994).

[23] I offer a much fuller account in *How the Law Responds to Self-Help*, which is cited above in note 18.

Doug Lichtman is a professor of law at the University of Chicago and can be reached via email at dgl@uchicago.edu. This piece is expanded from a shorter column first published in the February 2006 issue of IP Law & Business. For further analysis on point, see Doug Lichtman, *How the Law Responds to Self-Help*, 1 JOURNAL OF LAW, ECONOMICS, AND POLICY 215 (2005).