DRM {AND, OR, VS.} THE LAW

By Pamela Samuelson

Copyright industries are hoping that digital rights management (DRM) technologies will prevent infringement of commercially valuable digital content, including music and movies. These industries have already persuaded legislatures in the U.S., the European Union, and other countries to adopt broad anti-circumvention rules to protect DRM from being hacked, and courts have interpreted these statutes even more broadly than the lawmakers intended.

Some copyright industries now want DRM to be mandated in all digital media devices, either through standard-setting processes or through legislation. Though mandates for ubiquitous DRM are unlikely to be legislated soon, the threat of DRM mandates should be taken seriously. Computing professionals should be aware that private standard-setting processes may result in even less protection for consumer and other public interests than legislation that in the past has included at least some consumer-protection rules. U.S. Reps. Rick Boucher (D., VA), Zoe Lofgren (D., CA), and others, recognizing that DRM and overbroad anti-circumvention rules

The main purpose of DRM is not to prevent copyright infringement but to change consumer expectations about what they are entitled to do with digital content.

THE DMCA IMPEDES THE PROGRESS OF SCIENCE, is economically unjustifiable, and lacks the balance the Constitution requires of intellectual property legislation.

interfere with legitimate interests of consumers, have proposed legislation to safeguard these interests.

Computing professionals who want to contribute to more balanced intellectual property policy should do two things: collectively articulate the positive social benefits of general-purpose technologies to counteract proposed DRM mandates; and strongly support consumer-protection legislation for DRM-protected content (such as warning labels) and proposed reform of anti-circumvention rules.

DRM Goes Beyond Copyright

DRM is sometimes said to be a mechanism for enforcing copyrights [9]. While DRM systems can certainly prevent illegal copying and public distribution of copyrighted works, they can do far more; they can as easily prevent the copying and distribution of public-domain works as copyrighted works. Moreover, even though copyright law confers on copyright owners the right to control only public performances and displays of these works, DRM systems can also be used to control private performances and displays of digital content. DRM systems can thwart the exercise of fair use rights and other copyright privileges. DRM can be used to compel users to view content they would prefer to avoid (such as commercials and FBI warning notices), thus exceeding copyright's bounds.

Given that DRM permits content owners to exercise far more control over uses of copyrighted works than copyright law provides, the moniker "DRM" is actually a misnomer. These technologies are not really about the management of digital "rights" but rather about management of certain "permissions" to do X, Y, or Z with digital information. If DRM systems were about digital management of rights, they would need to be designed so users could express their rights under copyright, too. Thus far, digital rights expression languages (RELs) lack semantics to allow the expression of concepts like fair use [5]. DRM cannot accommodate user rights without REL vocabularies capable of expressing them. Even if RELs developed semantics to express user rights, content owners may abjure expressing them unless forced to do so by law or competition.

DRM is more aptly described as "code as code" [4]—a private governance system in which computer program code regulates which acts users are (or are not) authorized to perform—than as a rights management regime or as a copyright-enforcement mechanism. An alternative phrase for DRM is "digital restrictions management," given its use by copyright industries to restrict user rights [3]. Whether users ought to be able to circumvent DRM to exercise their rights has been the subject of some debate.

Anti-Circumvention Rules

In response to industry concern about the vulnerability of DRM technologies to hacking, the U.S. Congress in 1998 passed the Digital Millennium Copyright Act (DMCA) in order to outlaw certain acts of circumvention and technologies designed to circumvent technical measures used to protect copyrighted works; other countries have followed suit (see Dusollier's article in this issue). Section 1201(a)(1)(A) forbids circumvention of technical measures copyright owners use to protect access to their works. Section 1201(a)(2) forbids manufacture or distribution of technologies primarily designed or produced to circumvent access controls, while parallel provision 1201(b)(1) outlaws other circumvention technologies. Anyone injured by violation of these rules can sue for damages, injunctive relief, and attorney fees. Violating these rules willfully and for profit is a felony.

Circumvention is permissible for some purposes, such as achieving program-to-program interoperability and engaging in encryption research and computer security testing. However, the statutory exceptions are very drawn narrowly and fail to recognize many legitimate reasons for circumventing technical measures, including to engage in research about nonencryption-based watermarking technologies or analyze computer viruses or worms [6].

A careful study of the legislative history of the DMCA and the detailed structure of the anti-circumvention rules reveals that Congress intended for circumvention of copy- and use-controls to be lawful when performed for noninfringing purposes, such as to enable fair uses. Circumvention of access controls was treated differently by lawmakers on the theory that lawful access is a prerequisite for fair use rights.

Unfortunately, early decisions interpreting the DMCA, such as Universal City Studios v. Corley in 2000, have treated persistent access controls, such as the Content Scramble System (CSS) used in DVD players and discs, as access controls. Universal charged

Corley with violating 1201(a)(2) for posting a CSS decryption program known as DeCSS on his *2600* magazine's Web site as part of its news coverage of the controversy about DeCSS. By ruling that DeCSS was a 1201(a)(2) tool, not a 1201(b)(1) tool, the court implicitly ruled that circumventing CSS to make fair use of a DVD movie violates 1201(a)(1)(A).

In this and other respects, the Corley decision adopted the copyright industry's preferred interpretation of the DMCA as virtually unlimited in its protection of DRM. Subsequent decisions may correct some errors in the Corley decision, but for now it is a benchmark interpretation of the DMCA.

Constitutional challenges to DMCA anti-circumvention rules were unsuccessful in Corley, but many scholars of intellectual property law continue to doubt their constitutionality. Even though the Corley decision might suggest that Carnegie Mellon University researcher David Touretzky's Gallery of CSS Descramblers violates the law, the First Amendment of the U.S. Constitution would almost certainly protect his right to post this educational material on his Web site, as well as my right to link to this gallery on my course Web site.

Further challenges to the DMCA's rules may be fueled by the U.S. Supreme Court's recent decision in Eldred v. Reno. Even though the Court upheld the Copyright Term Extension Act (CTEA) of 1998, it did so because the life of the author plus 70 years was still a "limited time," as the Constitution requires, whereas the DMCA anti-circumvention protection is perpetual in duration. The CTEA added 20 years to the terms of existing copyrights, thereby thwarting the plans of Eric Eldred to publish works from the 1920s on the Web. Among the authors whose works are still in copyright thanks to the CTEA are Bela Bartok, Kahlil Gibran, Robert Frost, and Maurice Ravel. The DMCA impedes the progress of science, is economically unjustifiable, and lacks the balance the Constitution requires of intellectual property legislation.

DRM Mandates?

DRM can be mandated in two ways: through standard-setting processes or through public legislation. Illustrative of the former is the agreement reached in 1996 between the motion picture and consumer electronics industries about a standard technical measure for DVD players and discs—the CSS code Norwegian teenager Jon Johansen famously reverse-engineered in 1999. The motion picture industry had significant leverage in these negotiations because it owned key patents for DVD players. No firm can build a DVD player without licensing these patents, and no license is granted without agreement to embed CSS in the licensed DVD players.

The recording industry hoped to achieve a similar result in negotiations with makers of digital music players through the Secure Digital Music Initiative (SDMI), a consortium organized by the major labels who are members of the Recording Industry Association of America and that included representatives of makers of digital music players. These negotiations were unsuccessful for a number of reasons, including diverse interests of participants and weaknesses in watermarking technologies SDMI proposed as standards. Princeton University computer science professor Edward Felten, along with certain colleagues and some students, quickly discovered these weaknesses when SDMI challenged the hacker community to break them (see Felten's article in this issue). SDMI initially tried to suppress publication of Felten's paper about the weaknesses, claiming it was an illegal circumvention technology. After Felten sought a court declaration that he had a First Amendment right to publish, SDMI withdrew its objection.

Though the content industry must surely be pleased by recent DRM-friendly developments, such as Microsoft's Palladium initiative and the Trusted Computing Platform Alliance (TCPA) for embedding DRM into platform infrastructure, it must also worry about three things: Microsoft and TCPA firms cannot control every platform for playing, viewing, and copying digital content; competition among different DRMs may fragment the consumer market and suppress consumer demand; and as Johansen, Felten, and others have proved, no DRM technology is hacker-proof.

Mandating standard DRM technologies in digital media devices would address the first two. Sen. Ernest Hollings (D., SC) introduced the Consumer Broadband and Digital Television Promotion Act of 2002 (S. 2048), contemplating that representatives of copyright industries, makers of digital media devices, and consumer groups would have 12 months to reach agreement on a DRM standard. Even if no consensus emerged, the Hollings bill would give the Federal Communications Commission (FCC) authority to require digital media devices to embed whatever DRM technology the FCC selected as a standard. Thereafter, it would be both a civil wrong and a felony to make any digital media device without this DRM and/or to remove or tamper with it.

The Hollings bill has no immediate prospect of enactment, in part because several prominent members of Congress oppose it. But it is important to understand it is what some in the content industry really want and can be expected to pursue vigorously in Congress. There are already two U.S. precedents for mandating technical measures: the Audio Home

Recording Act (AHRA) of 1992, which requires installation of serial copy management system chips in all consumer-grade digital audiotape technologies; and the DMCA, which requires Macrovision's copy-control technology be installed in all post-1998 videocassette recording devices. Meanwhile, one or more "mini-Hollings" bills may soon be proposed to mandate DRM in particular devices; consider, for example, the proposal to mandate "broadcast flag" technology in digital televisions to mark the programs rights holders do not want users to copy. If Congress mandates standard DRMs through a series of such bills, it may eventually seem logical to adopt a more general mandate of DRM in digital media devices.

The content industry complains bitterly that the technology industry has been uncooperative with its efforts to control piracy through DRM. The Hollings bill is partly intended to give the content industry leverage in negotiations with the technology industry on DRM standards. The only way to preclude outsiders from developing technologies lacking an agreed-upon DRM standard would be legislation to mandate it. Privately negotiated DRM mandates are unlikely to accommodate fair uses, and once industry groups have agreed on a DRM standard, the public will have little leverage for demanding fair use accommodations.

Hopefully, consumer discontent with highly restrictive DRM MAY FORCE CONTENT OWNERS TO MAKE DRM MORE CONSUMER-FRIENDLY, though this remains to be seen.

The content industry cannot realistically expect DRM mandates to stop "darknet" (such as peer-to-peer file sharing) distribution of copyrighted content [1]. The main goal of DRM mandates is not, as the industry often claims, to stop "piracy" but to change consumer expectations. In the content industry's view, consumers don't have rights; they have expectations. Consumers may not like DRM systems, but if "legitimate" content is available only on this basis, they'll get used to it.

The technology industry and computing professionals can effectively oppose DRM mandates only by communicating to policymakers the positive virtues of general-purpose computers and other technologies with substantial noninfringing uses and the reasons DRM mandates would negatively affect competition, innovation, and other social values. This needs to be done soon, so Congress realizes that information technologies are useful for more than allowing users to engage in "piracy."

Consumer Protection

DRM mandates may seem inherently anti-consumer. However, AHRA allows consumers to make first-generation personal-use copies of digital audiotape (DAT) recordings, though they also have to pay a tax on DAT technologies for eventual distribution to copyright owners. Though the DMCA may have mandated installation of Macrovision's copy-control technology in videocassette recorders, it permits some home taping of digital content. The Hollings bill contemplates that consumer groups would be represented in negotiations about DRM standards and that some personal-use copying would be permissible.

Three exceptions to DMCA anti-circumvention rules respond to consumer interests. Nonprofit organizations can lawfully circumvent access controls to allow them to decide whether to buy DRM-protected content. Parents can circumvent DRMs to regulate what their children access. Individuals can also circumvent DRMs to protect against unauthorized collection of their personal data. The U.S. Library of Congress in 1999 conducted a rulemaking on the DMCA anti-circumvention rules that recognized the right of lawful users to circumvent broken access controls and assess software-filtering programs.

Thus, the law already provides some consumer protection, if weakly, for DRM technology. More is in the works. Rep. Rick Boucher recently introduced legislation in response to consumer frustration with copy-protected CDs. These CDs typically fail to warn consumers prior to purchase that: they are copy-protected; they may not play on their preferred digital media device; and the music may not be recordable on their personal computer. Boucher's Digital Media Consumers' Rights Act of 2002 (HR 107) would outlaw sale or distribution of digital music products without adequate labeling and direct the Federal Trade Commission to adopt rules about digital music product labeling.

The more widely DRM is deployed, the more likely are other consumer-protection rules (such as for user privacy) (see Cohen's article in this issue). Beginning in 2001, the European Union imposed an obligation on copyright owners to enable users to exercise certain copyright exceptions (see Dusollier's article in this issue). Even bolder is a proposal [2] to establish a "fair use infrastructure" for DRM-protected content under which content owners would have to deposit keys to DRM locks with an escrow agent, so fair users could obtain the keys when needed. Rep. Christopher Cox (R., CA) has endorsed digitalconsumer.org's "consumer bill of rights" by proposing a resolution to announce as "the sense of Congress" that consumers who legally acquire copyrighted works should be free to use them in various noncommercial ways, including to time- and space-shift, make backup copies, use the information on the platform of one's choice, and transform copies from one format to another. A fairer balancing of the interests of copyright owners and the public could be attained if DRM technologies had to accommodate these and other consumer rights.

Broader consumer protection in DRM will not happen overnight. Unless the technology industry, computing professionals, and public interest organizations define and endorse a common set of principles, it may not happen at all. But the content industry is deluded if it thinks there are no limits on the controls it can exercise over the uses of digital content. Hopefully, consumer discontent with highly restrictive DRM may force content owners to make it more consumer-friendly, though this remains to be seen.

Reforming the DMCA

Consumers, researchers, and other legitimate reverse engineers would benefit from enactment of the Digital Choice and Freedom Act of 2002 (HR 5522), co-sponsored by Reps. Zoe Lofgren and Mike Honda (D., CA). It states that "[c]ontrary to the intent of Congress, Section 1201 has been interpreted [in Corley] to prohibit all users—even lawful ones—from circumventing technical restrictions for any reason. As a result, the lawful consumer cannot legally circumvent technological restrictions, even if he or she is simply trying to exercise a fair use or to utilize the work on a different media device."

To restore the balance Congress intended to achieve with the DMCA and repudiate restrictive interpretations (such as Corley), the Digital Choice Act would allow lawful acquirers of copyrighted material to circumvent technical measures if necessary to make noninfringing uses of the work if the copyright owner has not made publicly available the necessary means to permit the noninfringing uses without additional cost or burden to users. Moreover, the Digital Choice Act would permit users to make and distribute technologies necessary to enable noninfringing uses of copyrighted works.

The Digital Media Consumers' Rights bill discussed earlier takes a slightly different approach but has a similar goal. It would make circumvention lawful as long as it does not result in copyright infringement. Like the Lofgren-Honda bill, it would allow the manufacture and distribution of technologies capable of enabling significant noninfringing uses of copyrighted works. It would further amend the DMCA's anti-tool rules to immunize tool making in furtherance of scientific research about technical measures.

Conclusion

This article is entitled "Digital Rights Management {and, or, vs.} the Law" because DRM has more than one potential relationship with the law: it can enforce, displace, and override legal rights, while the law can constrain the design of DRM.

How DRM and the law interact over the next decade depends on decisions made in the near future by individual technologists, firms in the technology and content industries, participants in standard-setting processes, and legislators and other policymakers. DRM technology is not policy neutral but highly policy charged, in part because of the goals the content industry has for it.

It may seem obvious to computing professionals why DRM should not be mandated in digital media devices and why consumers, scientists, and other legitimate reverse-engineers ought to be able to continue to engage in fair and other noninfringing uses of copyrighted works. Unfortunately, it is not as obvious to members of Congress and other policymakers. Computing professionals can make a positive difference in the policy debates over DRM—if they choose to do so. C

References

1. Biddle, P., England, P., Peinado, M., and Willman, B. The darknet and the future of content distribution. In *Proceedings of the 2002 ACM Workshop on Digital Rights Management* (Washington, DC, Nov. 18, 2002).
2. Burk, D. and Cohen, J. Fair use infrastructure for rights management systems. *Harvard J. Law & Tech. 15* (2001), 41–83.
3. Free Software Foundation. *Some Confusing or Loaded Words and Phrases That Are Worth Avoiding*; see www.gnu.org/philosophy/words-to-avoid.html.
4. Lessig, L. *Code and Other Laws of Cyberspace.* Basic Books, NY, 2000.
5. Mulligan, D. and Burstein, A. Implementing copyright limitations in rights expression languages. In *Proceedings of the 2002 ACM Workshop on Digital Rights Management* (Washington, DC, Nov. 18, 2002).
6. Samuelson, P. Intellectual property and the digital economy: Why the anti-circumvention rules need to be revised. *Berkeley Tech. Law J. 14* (1999).
7. Stefik, M. Shifting the possible: How trusted systems and digital property rights challenge us to rethink digital publishing. *Berkeley Tech. Law J. 12* (1997).

Pamela Samuelson (pam@sims.berkeley.edu) is a Chancellor's Professor of Law and Information Management at the University of California at Berkeley and Director of the Berkeley Center for Law & Technology.

This work is supported through National Science Foundation Grant No. SES 9979852.