Digital Rights Management {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, such as music and movies. These industries have already persuaded legislatures to adopt broad anti-circumvention rules to protect DRM from being hacked, and courts have interpreted these statutes even more broadly than legislators intended.

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 of consumer and other public interests than legislation which in the past has included at least some consumer protection rules. Some legislators who recognize that DRM and overbroad anti-circumvention rules interfere with legitimate interests of consumers have proposed legislation to safeguard these interests.

If computing professionals want to contribute to more balanced intellectual property policy, they should do two things: First, they should collectively articulate the positive social benefits of general purpose technologies to counteract proposed DRM mandates. Second, they should strongly support consumer protection legislation for DRM-protected content, such as warning labels, and proposed reforms of anti-circumvention rules.

DRM GOES BEYOND COPYRIGHT

DRM is sometimes said to be a mechanism to enforce copyrights.[9] While DRM systems can certainly prevent illegal copying and public distribution of copyrighted works, these systems can do far more than this. DRM technologies can as easily prevent copying and distribution of public domain works as copyrighted ones. Furthermore, 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, 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 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," then they would need to be designed so that users could express their rights under copyright too. Thus far, digital rights expression (REL) languages lack semantics to allow concepts like fair use to be expressed.[7] 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"[6]—a private governance system in which computer program code regulates which acts users are authorized to do (or not)—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.[5] Whether users ought to be able to circumvent DRM to exercise their rights has been the subject of some debate.

ANTI-CIRCUMVENTION RULES PROTECT DRM

In response to industry concerns about the vulnerability of DRM technologies to hacking, the U.S. Congress passed the Digital Millennium Copyright Act (DMCA) that outlaws certain acts of circumvention and technologies designed to circumvent technical measures used to protect copyrighted works. Other countries have followed suit.[4] Section 1201(a)(1)(A) forbids circumvention of technical measures copyright owners used 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 be sued 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 or engaging in encryption research and computer security testing. However, the statutory exceptions are very narrowly drawn and fail to recognize many legitimate reasons for circumventing technical measures, such as to engage in research about non-encryption-based watermarking technologies and to analyze computer viruses or worms.[8]

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 done for non-infringing purposes, such as to enable fair uses. (Circumvention of access controls was treated differently 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*, have treated persistent access controls, such as the Content Scramble System (CSS) used in DVD players and disks as access controls. Universal charged Corley with violating 1201(a)(2) for posting a CSS decryption program known as DeCSS on his magazine's website as part of 2600's 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 the 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 Touretsky's Gallery of CSS Descramblers violates the DMCA, the First Amendment would almost certainly protect his right to post this educational material on his website, as well as my right to link to this gallery on my course website.

Further challenges to the DMCA rules may occur if the Supreme Court strikes down the Copyright Term Extension Act of 1998 in *Ashcroft v. Eldred*. The CTEA added 20 years to the terms of existing copyrights, thereby thwarting the plans of Eric Eldred to publish works from the 1920's on the Web. Many arguments raised against the CTEA also apply to the DMCA. Like the CTEA, the DMCA impedes the progress of science, is economically unjustifiable, and lacks balance that the Constitution requires of intellectual property legislation.

ARE DRM MANDATES NEXT?

DRM can be mandated in two ways: through standard-setting processes or through public legislation. Illustrative of the former is the agreement reached between the motion picture and consumer electronics industries about a standard technical measure for DVD players and disks—the CSS code which Norwegian teenager Jon Johansen so famously reverse engineered. 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 will be 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). These negotiations were unsuccessful for a number of reasons, including diverse interests of participants and weaknesses in watermarking technologies SDMI proposed as standards. Princeton Professor Edward Felten, certain colleagues, and some students quickly discovered these weaknesses when SDMI challenged the hacker community to break them. 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 the paper, SDMI withdrew its objection to the publication.

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

Mandating standard DRM technologies in digital media devices would address the first two concerns. Senator Hollings' Consumer Broadband and Digital Television Promotion Act of 2002 (S. 2048) contemplates that representatives of copyright industries, makers of digital media devices, and consumer groups would have twelve months to reach agreement on a DRM standard. Even if no consensus emerged, the Hollings bill would give the Federal Communications Commission 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 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, first, that the Hollings bill is what the content industry really wants, and it can be expected to pursue this goal vigorously in Congress. Second, there are already two U.S. precedents for mandating technical measures. The Audio Home Recording Act (AHRA) requires installation of serial copy management system chips in all consumer-grade digital audio tape technologies, and the DMCA requires Macrovision's copy-control technology to be installed in all post-1998 video cassette recording devices. Third, 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 programs that rights-holders do not want users to copy. If Congress mandates standard DRMs through a series of "mini-Hollings" 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 any 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 upon a DRM standard, the public will have little leverage for demanding fair use accommodations.

The content industry cannot realistically expect DRM mandates to stop "darknet" distribution of copyrighted content.[1] The main goal of DRM mandates is not, as the industry so often claims, to stop "piracy," but to change consumer expectations. In the content industry's view, consumers don't have rights; they only have expectations.

Consumers may not like DRM systems, but if the only "legitimate" content is available on this basis, consumers will get used to it.

The technology industry and computing professionals can only effectively oppose DRM mandates by communicating to policymakers the positive virtues of general-purpose computers and other technologies with substantial non-infringing uses and the reasons DRM mandates would negatively impact competition, innovation, and other social values. This needs to be done soon.

CONSUMER PROTECTION

DRM mandates may seem inherently anti-consumer. However, the AHRA supported the right of consumers to make first generation personal use copies of DAT recordings, although they had to pay a tax on DAT technologies for eventual distribution to copyright owners. The DMCA may have mandated installation of Macrovision's copy-control technology in VCRs, but it permits some home taping of digital content. The Hollings bill discussed above 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. Non-profits can lawfully circumvent access controls to enable them to decide whether to buy DRM-protected content. Parents can circumvent DRMs to regulate what their children are accessing. Individuals can also circumvent DRMs to protect against unauthorized collection of personal data about them. The Library of Congress conducted a rulemaking on the DMCA anti-circumvention rules that recognized the right of lawful users to circumvent broken access controls and to assess software filtering programs.

Thus, the law already provides some consumer protection, if weakly, of DRM technology. More is in the works. Representative Rick Boucher of Virginia has recently introduced legislation to respond to consumer frustration with copy-protected CDs. These CDs typically fail to warn consumers prior to purchase that the CD is copy-protected, that the disk may not play on the consumers' preferred digital media device, and that the music may not be recordable on the consumer's personal computer. Boucher's Digital Media Consumers' Rights Act of 2002 (HR 5544) 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 become other consumer protection rules, such as protections of user privacy.[3] The EU has already imposed an obligation on copyright owners to enable users to exercise certain copyright exceptions.[4] Even bolder is a proposal 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 that fair users could obtain the keys when needed.[2] Congressman Cox of California 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 non-commercial ways, including to time-shift, 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 of DRM will not happen overnight, and unless the technology industry, computing professionals, and public interest organizations get organized, it may not happen at all. In my view, the content industry is deluded if it thinks there are no limits on the controls it can exercise over uses of digital content. Hopefully, consumer discontent with highly restrictive DRM may force content owners to make DRM more consumer-friendly, but 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), cosponsored by Silicon Valley Representatives Zoe Lofgren and Mike Honda. 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 that Congress intended to achieve with the DMCA and to 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 non-infringing uses of the work if the copyright owner has not made publicly available the necessary means to permit the non-infringing uses without additional cost or burden to users. The Digital Choice Act would, moreover, permit users to make and distribute technologies necessary to enable non-infringing uses of copyrighted works.

The Digital Media Consumers' Rights bill discussed previously takes a slightly different approach, but with 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 making and distribution of technologies capable of enabling significant non-infringing uses of copyrighted works. It would further amend the anti-tool rules of the DMCA to immunize tool-making in furtherance of scientific research about technical measures.

CONCLUSION

This article is entitled "DRM {and, or, versus} the law" because DRM has more than one potential relationship with the law: It can enforce legal rights; it can displace legal rights; it can override legal rights; and the law can constrain the design of DRM.

How DRM and the law will interact will depend heavily on decisions made in the near future by individual technologists, by firms in the technology and content industries, by participants in standard-setting processes, by legislators, and by other policymakers. DRM technology is not policy-neutral, but highly policy-charged, in part because of content industry goals 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 non-infringing 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.

Pamela Samuelson 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. The author is grateful for research support from NSF Grant No. SES 9979852. She can be reached at pam@sims.berkeley.edu.

Footnotes

[1] Biddle, P, P. England, M. Peinado, & B. Willman. The Darknet and the Future of Content Distribution. Proceedings of 2002 ACM Workshop on Digital Rights Management.

[2] Burk, D. L. & Julie E. Cohen. Fair Use Infrastructure for Rights Management Systems. Harvard Journal of Law and Technology, 15: 41-83 (2001).

[3] Cohen, J. DRM and Privacy, Comm. ACM 46:xx (2003) [article in this issue]

[4] Dusollier, S. Fair Use by Design in the European Directive, Comm. ACM 46:xx (2003) [article in this issue]

[5] Free Software Foundation. Some Confusing or Loaded Words and Phrases That are Worth Avoiding, available at http://www.gnu.org/philosophy/words-to-avoid.html.

[6] Lessig, L. Code and Other Laws of Cyberspace (2000).

[7] Mulligan, D. and A. Burstein. Implementing Copyright Limitations in Rights Expression Languages. Proceedings of 2002 ACM Workshop on Digital Rights Management.

[8] Samuelson, P. Intellectual Property and the Digital Economy: Why the Anti-Circumvention Rules Need to be Revised, Berkeley Tech. L.J. 14:519 (1999).

[9] Stefik, M. Shifting the Possible: How Trusted Systems and Digital Property Rights Challenge Us to Rethink Digital Publishing. Berkeley Tech. L.J. 12:137 (1997)