FOREWORD

By C.J. Alice Chen[†] *& Aaron Burstein*[‡]

The controversy surrounding digital rights management ("DRM") is the most recent episode, still being played out, in the tension between copyright protection and new technology. This begets a further tension between the role of public, as opposed to private, decisionmaking in determining how to regulate this technology. A backdrop for this debate is the set of potential advantages that inexpensive computing devices and high-speed networks present for the preservation and distribution of information; these advantages have been well studied in recent years. On the other hand, the rapid, unauthorized distribution of flawless digital copies poses a threat to established copyright-based businesses that has received much attention in recent years.[1] The idea of building copy restrictions into software and hardware emerged as a common response to such sundry problems as the unauthorized copying of software,[2] music,[3] and movies.[4] What has varied is the extent to which changes in the law, sometimes as drastic as technological mandates, prescribed and protected such technological controls. This interaction between law and technology lies at the heart of much of the DRM debate.

Before going further in the introduction of this debate, it is helpful to state a definition of DRM. Here, too, there is no general agreement; some regard the phrase "digital rights management" to mean "the digital man-

---

† Editor-in-Chief, Berkeley Technology Law Journal; J.D. Candidate, 2003, Boalt Hall School of Law, University of California, Berkeley; B.A., Molecular Cell Biology & English Literature, University of California, Berkeley, 2000.

‡ J.D. Candidate, 2004, Boalt Hall School of Law, University of California, Berkeley; M.S., University of California, Berkeley, 1998; Sc.B., Brown University, 1996.

1. *See generally* COMM. ON INTELL. PROP. RIGHTS & EMERGING INFO. INFRASTRUCTURE, NAT'L RESEARCH COUNCIL, THE DIGITAL DILEMMA: INTELLECTUAL PROPERTY IN THE INFORMATION AGE (Nat'l Academy Press, *available at* http://books.nap.edu/books/0309064996/html/2.html#pagetop, 2000).

2. Vault Corp. v. Quaid Software, Ltd., 847 F.2d 255 (5th Cir. 1988).

3. Audio Home Recording Act of 1992, Pub. L. No. 102-563, 106 Stat. 4237 (1992) (codified at 17 U.S.C. §§ 1001-1010) [hereinafter AHRA] (creating standards for copy controls, and requiring the incorporation of such copy controls, on digital audio recording devices); Recording Indus. Ass'n v. Diamond Multimedia Sys., 180 F.3d 1072 (9th Cir. 1999) (discussing the requirements for digital audio home recording devices under the AHRA).

4. *See* Universal City Studios, Inc. v Reimerdes, 111 F. Supp. 2D 294, 308 (S.D.N.Y. 2000) (describing the access control technology that protects the contents of DVDs).

agement of rights," while others take it to mean "the management of digital rights."[5] Despite this interpretive controversy, it is possible to distill some of the common features of systems that are assigned the DRM label. Generally speaking, DRM systems consist of "secure packaging and delivery software designed to prevent purchasers and third parties from making unauthorized uses of digital works."[6] In other words, DRM systems provide a means of expressing usage rules, a means of associating those rule with content, and frequently, a means of enforcing these rules by preventing actions that the usage rules do not explicitly permit.[7] The DRM system that underlies the now-familiar DVD, for example, enforces a "view-only" rule by encrypting the movies and requiring that device manufacturers, who must license patents necessary to implement the DVD encryption algorithm, refrain from including means for copying in their products.

DRM systems that are currently under development promise two major advances from the rather coarse rules of early DRM. First, "rights expression languages" have the potential for the expression of an increased variety of nuanced usage rules by rights holders.[8] Second, modifications to the basic architecture of the Intel-based personal computer platform could provide a "trusted" environment in which to run DRM components. This

---

5. Renato Ianella, *Digital Rights Management (DRM) Architectures*, D-LIB MAGAZINE (June 2001), *at* http://www.dlib.org/dlib/june01/iannella/06iannella.html. Ianella writes:

> Previously, Digital Rights Management (DRM) focused on security and encryption as a means of solving the issue of unauthorized copying, that is, lock the content and limit its distribution to only those who pay. . . . The second-generation of DRM covers the description, identification, trading, protection, monitoring and tracking of all forms of rights usages over both tangible and intangible assets including management of rights holders relationships.

Id.

6. Dan L. Burk & Julie E. Cohen, *Fair Use Infrastructure for Rights Management*, 15 HARV. J. LAW & TECH. 41, 48 (2001).

7. This method of decisionmaking—disallowing everything that is not explicitly permitted—is an embodiment of the "closed-world assumption" that is familiar to many technologists. *See* Barbara L. Fox & Brian A. LaMacchia, *Encouraging Recognition of Fair Uses in DRM Systems*, COMMUNICATIONS OF THE ACM (Apr. 2003) at 61, 61, *available at* http://delivery.acm.org/10.1145/650000/641233/p61-fox.pdf?key1=641233&key2=2926712501&coll=ACM&dl=ACM&CFID=10296420&CFTOKEN=18029193.

8. One such rights expression language, the Open Digital Rights Language (ODRL), defines a vocabulary for time-limited usage permissions, pay-per-use conditions, and permission for users to transfer their usage rights to other users. *See* IPR Systems Pty Ltd., *Open Digital Rights Language (ODRL) Specification*, (Renato Ianella, ed., Aug. 8, 2002) 8-15, *at* http://odrl.net/1.1/ODRL-11.pdf (last visited May 5, 2003).

trusted environment would prevent users from performing operations, which current PCs allow, that result in the unauthorized copying of decrypted content.

DRM systems are not, of course, free-standing technologies intended to control the use of copyrighted works. Instead, DRM systems fall within the category of "technological protection measures" that the Digital Millennium Copyright Act (DMCA)[9] explicitly protects against circumvention.[10] Congress' stated goal, in granting copyright holders a right of access to their works, was to promote the emerging role of digital technology in commerce[11] without "affect[ing] rights, remedies, limitations, or defenses to copyright infringement, including fair use."[12] The DMCA itself, however, does not prescribe any technological safeguards of these rights, remedies, limitations, and defenses, nor does it excuse users who circumvent access controls to make lawful use of copyrighted content.[13] The DMCA thus grants copyright holders broad leeway to encode access and usage policies into DRM systems that may effect a balance of rights quite different from the one found within traditional copyright law.[14]

---

9. 17 U.S.C. §§ 101-1205 (2000).

10. *See* 17 U.S.C. § 1201(a)(1)(A) (prohibiting the act of circumventing a "technological measure that effectively controls *access* to a work protected under" Title 17) (emphasis added); 17 U.S.C. § 1201(a)(2) (prohibiting the manufacture and distribution of access control circumvention devices); 17 U.S.C. § 1201(b) (prohibiting manufacturing or trafficking in devices "primarily designed or produced for the purpose of circumventing protection afforded by a technological measure that effectively protects a right of a copyright owner" under the Title 17).

11. H.R. REP. NO. 105-551, pt. 1, at 18 (1998) (citing a goal of "maintain[ing] strong protection for intellectual property and promot[ing] the development of electronic commerce and the technologies to support that commerce").

12. 17 U.S.C. § 1201(c)(1). *See also* 17 U.S.C. § 1201(c)(2) (specifying that section 1201 does not affect the scope of contributory or vicarious liability); 17 U.S.C. § 1201(c)(4) (stating that section 1201 does not "enlarge or diminish any rights of free speech or the press for activities using consumer electronics, telecommunications, or computing products"); 17 U.S.C. § 1201(d)-(h) (granting specific exceptions to section 1201's anti-circumvention provisions); 17 U.S.C. § 1201(a)(1)(C) (directing the Librarian of Congress to conduct a trienniel rulemaking to determine whether more (or fewer) exceptions are necessary to relieve users "adversely affected" by sections 1201(a)(1)(A) and 1201(a)(1)(B)).

13. *Accord* Universal City Studios, Inc. v. Corley, 273 F.3d 429 (2d Cir. 2001).

14. The Supreme Court recently addressed part of this overall balance, that between copyright and the First Amendment, in *Eldred v. Ashcroft*, 123 S. Ct. 769 (2003). In *Eldred*, the Court noted that the idea/expression dichotomy and the "'fair use' defense" are hallmarks of the "definitional balance between the First Amendment and the Copyright Act." *Id*. at 788-89. The *Eldred* Court did not locate, however, other points on "the traditional contours of copyright protection." *Id*. at 790.

Legislative protection of privately determined copyright terms is not, however, an entirely new chapter in the history of copyright. The DRM systems protected under the DMCA fit into a progression of technological, legislative, and legal events, that date back at least as far as the Betamax decision in 1984.[15] *Sony* brought to the forefront the potential for inexpensive consumer electronics to turn ordinary consumers into copyright infringers, though the Supreme Court held otherwise. When digital audio tape ("DAT") recorders began to emerge—and with it the possibility that every purchaser of a DAT recorder could make digital copies of musical recordings—the recording industry sought to prohibit the importation of DAT recorders altogether. Eventually, recording companies, artists, composers, and electronics manufacturers reached a "carefully negotiated compromise"[16]—a DRM solution—that was mandated in the Audio Home Recording Act. In brief, the Act directed electronics manufacturers to incorporate the Serial Copy Management System (or its equivalent)[17] into their devices to ensure that only one generation of digital copies could be made,[18] and banned devices whose "primary purpose" was to "avoid, bypass, remove, deactivate, or otherwise circumvent" the copy management system.[19] An agreement upon a technical standard achieved by industry groups thus attained the status of law. Despite this agreement, DAT devices did not become popular in the United States. Some commentators blame this mandatory DRM system for the poor sales of DAT devices,[20] while others point to the fact that the class of devices to which the Act applied did not include computers or—unimagined at the time the Act was passed—MP3 players.[21]

Such agreements have not always depended upon Congressional action. The DVD provides a prime example. The Content Scramble System (CSS) that is used to encrypt[22] the contents of DVDs is defined in a pro-

15. *See generally* Universal City Studios, Inc. v. Sony Corp., 464 U.S. 417 (1984).

16. Recording Indus. Ass'n v. Diamond Multimedia Sys., Inc., 180 F.3d 1072, 1078 n.6 (9th Cir. 1999).

17. 17 U.S.C. § 1002(a) (2000).

18. *See* Mitsui, *Serial Copy Management System (SCMS)*, at http://www.mitsuicdrstore.com/SCMS_nh.html (last visited May 2, 2003).

19. 17 U.S.C. § 1002(c).

20. *See* JESSICA LITMAN, DIGITAL COPYRIGHT 60 (2001).

21. *See* David Nimmer, *Back From the Future: A Proleptic Review of the Digital Millennium Copyright Act*, 16 BERKELEY TECH. L.J. 855, 867 (2001) (noting that the rapid development of technology made portable MP3 players, which were exempt from the Audio Home Recording Act's copy control mandate, unforeseeable at the time that the Act was passed).

22. Encryption is the process of "mathematically scrambling [data] so that only the two endpoints [of a communication] know how to read it." ERIC GREENBERG, NETWORK

prietary technical standard whose licensing is controlled by the DVD Copy Control Association (DVD CCA); Congress played no role in defining or mandating CSS. Two factors have maintained the viability of CSS as a means of preventing unauthorized copying. First, implementations of CSS require a license, which the DVD CCA alone controls.[23] Second, a group of motion picture studios prevailed in a lawsuit to enjoin the distribution of unauthorized decoding programs.[24] The law that facilitated this suit was not specific to the matter of motion picture encryption, of course; the studios brought their suit under the DMCA. The DMCA, in contrast to the Audio Home Recording Act, is not technology-specific and does not require DRM systems to provide users with any default rights.

The DMCA thus lays much of the groundwork for the privately determined terms under which ordinary users may use copyrighted works, and it is this broad latitude to set and enforce these rules through DRM systems that has prompted many of the concerns about (and defenses of) DRM. There is widespread agreement that the deterministic usage rules and "closed-world" model[25] of DRM systems clash with several of the limitations on copyright holders' exclusive rights. Fair use[26] is the most prominent example of this basic incompatibility. Unless DRM systems include a "judge on a chip,"[27] they will remain incapable of determining whether a user is copying part of a work for purposes of piracy or parody. This difficulty is not unique to fair use, though. The usage rules that DRM systems enforce do not necessarily honor exceptions for copying by libraries, the post-first sale loss of the right to distribute copies, backups of computer software, or exceptions for the disabled. Although these parts of copyright law pose exactly the same challenge that fair use does, there is still no way for a computer to discern the intent of a user. Making a backup copy of a computer program, as § 117(a) permits, involves the same operations as making an infringing copy.

The risk that a copyright holder would assume in granting such permissions to users has led to a variety of proposed solutions. On the one hand, Representative Zoe Lofgren (D-California) suggests relaxing the

---

APPLICATION FRAMEWORKS: DESIGN AND ARCHITECTURE 31 (1999).

23. Pavlovich v. Superior Court, 29 Cal. 4th 262, 266-67 (2002).

24. Universal City Studios, Inc. v. Reimerdes, 111 F. Supp. 2d 294 (S.D.N.Y. 2000), *aff'd sub nom.* Universal City Studios, Inc. v. Corley, 273 F.3d 429 (2d Cir. 2001).

25. *See* text accompanying note 7, *supra*.

26. 17 U.S.C. § 107 (2000).

27. Edward W. Felten, *A Skeptical View of DRM and Fair Use*, COMMUNICATIONS OF THE ACM (Apr. 2003) at 57, 58, *available at* http://delivery.acm.org/10.1145/650000/641232/p56-felten.pdf?key1=641232&key2=0949712501&coll=ACM&dl=ACM&CFID=10297022&CFTOKEN=48631939.

DMCA's ban on acts of circumventing access controls for non-infringing purposes as one way to permit users to experience works in ways that were not foreseen at the time of purchase.[28] On the other hand, others have suggested that altering the DMCA to limit copyright holders' ability to prosecute circumventors of DRM systems would gut the DMCA's protections and demolish most of the incentive that copyright holders have for making their works available in digital form. The benefits of new technologies, according to this view, overwhelm the benefits of standing limitations on copyright, thus demanding that DRM systems incorporate any of these exceptions is misguided. Given the widespread skepticism about the feasibility of faithfully including these exceptions in a DRM system, there may not be even a theoretical accommodation of fair use within a DRM system. One can also imagine a middle route: an agreement between copyright holders and users as to a set of "default" permissions for movies, music, books, and so on, ranging from allowing users to circumvent DRM systems to leaving the allocation of these rights entirely to the market. Still others advocate different means of addressing these rights.

DRM also raises concerns that are not directly related to copyright law, but rather are implicated by the technology that is required to build DRM systems. The loss of individual privacy is one interest that some commentators perceive DRM to threaten. In this Issue, for example, Julie Cohen writes that "[t]he future of privacy is increasingly linked to the future of copyright enforcement."[29] Others argue, however, that the amount and quality of personal information that DRM systems require from users is only marginally different from what is required by other forms of electronic commerce.[30] Indeed, as Lon Sobel argues, a potential trade-off for the collection of personal information might be a new compulsory licensing scheme—a distribution-based royalty, set by copyright holders, might reduce the incentive to deploy strong DRM controls.[31]

Others fear that DRM systems will create new risks to computer security. Some of the key technologies envisioned as parts of DRM systems—public key encryption and watermarking—still involve open research questions. Some technologists therefore feel that deploying these technologies now will prevent them from being studied openly, while at the same time the DMCA and other laws may not discourage attacks from

28. *See* Digital Choice and Freedom Act of 2002, H.R. 5522, 107th Cong. (2002) (introduced Oct. 2, 2002, by Rep. Zoe Lofgren from the sixteenth district of California).

29. Julie E. Cohen, *DRM and Privacy*, 18 BERKELEY TECH. L.J. 575, 575 (2003).

30. *See generally* Lionel S. Sobel, 18 BERKELEY TECH. L.J. 667 (2003).

31. *Id.* at 678-79.

parties whose motivations may be less than benign.[32] Further complicating the security concerns is the economics of DRM. Every digital copy of a work is as valuable as the original, yet the unit cost of security must remain low.[33] This could create the temptation for copyright holders to adopt, or even for Congress or the FCC to mandate, DRM systems that are not "robust" against attacks. The result, as Symposium panelist David Farber noted, may be that the FBI will end up investigating intellectual property crimes that better technology might have prevented.[34]

Finally, just as DRM technology that is confined to discrete hardware or software components is less effective than DRM technology that is integrated into a computing platform, so are national laws less effective than internationally harmonized laws, in protecting copyrighted works and DRM systems. Achieving this harmony, however, is a difficult task. Member states of the European Union, for example, have been slow to pass laws that implement the EC Copyright Directive of 2001 ("Directive"),[35] and the risk that one nation's implementing legislation will vary from another's is ever present.[36] The Directive also differs from the DMCA by addressing the prohibition on the circumvention of all DRM measures together,[37] rather than distinguishing between access controls and "rights controls."[38]

The European approach to limitations on copyright exclusivity also differs significantly from that of the DMCA. Part of the Directive permits

---

32. *See* Digital audio recording: Comments of Drew Dean at Symposium on the Law & Technology of Digital Rights Management: Tutorial on DRM Technology, co-sponsored by the *Berkeley Technology Law Journal*, Berkeley Center for Law & Technology, the Samuelson Law, Technology & Public Policy Clinic and the School of Information Management & Systems (Feb. 27-Mar. 1, 2003), *available at* http://www.law.berkeley.edu/institutes/bclt/drm/audio.html (last visited May 6, 2003).

33. Ordinarily, the cost of security scales with value of the work to be protected.

34. *See* Comments of David Farber, *Edited & Excerpted Transcript of the Symposium on the Law & Technology of Digital Rights Management*, 18 BERKELEY TECH. L.J. 697, 703-05 (2003).

35. Directive 2001/29/EC of the European Parliament on the Harmonisation of Certain Aspects of Copyright and Related Rights in the Information Society, 2001 O.J. (L. 168) 10, *available at* http://europa.eu.int/smartapi/cgi/sga_doc?smartapi!celexapi!prod!CELEXnumdoc&lg=en&numdoc=32001L0029&model=guichett (last visited May 6, 2003) [hereinafter EU Copyright Directive].

36. *See* Comments of Graeme Dinwoodie, *Edited & Excerpted Transcript of the Symposium on the Law & Technology of Digital Rights Management*, 18 BERKELEY TECH. L.J. 697, 763-67 (2003).

37. *Id*.

38. *Compare* 17 U.S.C. § 1201(a)(1)(A) (2000) (prohibiting the act of circumventing access controls only) *with* 17 U.S.C. § 1201(b) (banning traffic in rights control devices, but not the act of circumventing rights controls).

member states to "make available to the beneficiary of an exception or limitation . . . the means of benefiting from that exception or limitation" when the copyright holder has failed to do so.[39] The DMCA reposes all protection for copyright limitations in the lack of a prohibition on circumventing rights controls.[40] As Tony Reese argues, the DMCA provides incentives for copyright holders to "merge" rights controls and access controls within a DRM system.[41] This incentive, as Symposium speaker Graeme Dinwoodie noted, could have an anti-circumvention effect similar to that of the Directive, only without the Directive's provision of exercising exceptions.[42] Furthermore, this structure of the DMCA may render too many lawful uses off limits to the ordinary user.

On February 27, 2003 through March 1, 2003, the *Berkeley Technology Law Journal* co-sponsored a Symposium with the Berkeley Center for Law & Technology, the Samuelson Law, Technology & Public Policy Clinic and the School of Information Management & Systems, addressing all of the above issues regarding the current state and future direction of the legal and technological landscape of DRM.

The symposium began with a tutorial on DRM technology, by representatives from SRI International and Microsoft Corporation, followed by a tutorial on the legal and policy issues related to DRM, by Professor Pamela Samuelson. The second day of the symposium started with a panel discussing DRM as an enabler of new business models, followed by a second panel on the impacts of DRM on innovation, competition and security. The day concluded with discussions about the impacts of DRM on flows of information and on consumers.

Congresswoman Zoe Lofgren (D-California) started off the final day with the David Nelson Memorial Keynote Address, emphasizing the importance of raising awareness about DRM, and defects in the Digital Millenium Copyright Act, both with the public and with Congress. Following the keynote speech, Professor Pamela Samuelson moderated a panel on legal and policy issues related to DRM, and the Symposium concluded with a discussion of U.S. and foreign anticircumvention regulations, moderated by Professor Mark Lemley.

This Issue reflects the rich, ground-breaking content that was presented and discussed at the Symposium.

---

39. EU Copyright Directive, *supra* note 35, art. 6(4).

40. *See* 17 U.S.C. § 1201(b).

41. *See generally* R. Anthony Reese, *Legal Incentives for Adopting Digital Rights Management Systems: Merging Access Controls and Rights Controls*, 18 BERKELEY TECH. L.J. 619 (2003).

42. *See* Comments of Graeme Dinwoodie, *supra* note 36, at 762-66.