18:2 BERKELEY TECHNOLOGY LAW JOURNAL

The Law & Technology of Digital Rights Management Symposium

2003

Pages
487
to
771

Production: Produced by members of the *Berkeley Technology Law Journal* on PC computers. All editing and layout is done using Microsoft Word.

Printer: Joe Christensen, Inc., Lincoln, Nebraska.
Printed in the U.S.A.
The paper used in this publication meets the minimum requirements of American National Standard for Information Sciences—Permanence of Paper for Library Materials, ANSI Z39.48—1984.

Berkeley Technology Law Journal
University of California, Berkeley
Boalt Hall School of Law
587 Simon Hall
Berkeley, California 94720-7200
(510) 643-6454 (Phone)
(510) 643-6816 (Fax)
btlj@law.berkeley.edu

BERKELEY TECHNOLOGY LAW JOURNAL

VOLUME 18 NUMBER 2 SPRING 2003

TABLE OF CONTENTS

SYMPOSIUM: THE LAW & TECHNOLOGY OF DIGITAL RIGHTS MANAGEMENT

DONORS

The *Berkeley Technology Law Journal* acknowledges the following generous donors to Boalt Hall's Law and Technology Program:

Benefactors ($25,000 and above)

COOLEY GODWARD LLP
San Francisco, CA

FARELLA BRAUN + MARTEL LLP
San Francisco, CA

FENWICK & WEST LLP
Palo Alto, CA

GRAY CARY WARE & FREIDENRICH, LLP
Palo Alto, CA

HELLER EHRMAN WHITE & MCAULIFFE LLP
San Francisco, CA

LATHAM & WATKINS
San Francisco, CA

MILBANK, TWEED, HADLEY & MCCLOY LLP
Palo Alto, CA

MORRISON & FOERSTER LLP
San Francisco, CA

SKADDEN, ARPS, SLATE, MEAGHER & FLOM LLP
Palo Alto, CA

WEIL, GOTSHAL & MANGES LLP
Redwood Shores, CA

Members ($10,000 to $24,999)

ALSCHULER GROSSMAN STEIN & KAHAN LLP
Los Angeles, CA

BROBECK, PHLEGER & HARRISON LLP
Palo Alto, CA

COVINGTON & BURLING
San Francisco, CA

DAY CASEBEER MADRID & BATCHELDER LLP
Cupertino, CA

FINNEGAN, HENDERSON, FARABOW, GARRETT & DUNNER, L.L.P.
Palo Alto, CA

FISH & RICHARDSON P.C.
Menlo Park, CA

GIBSON, DUNN & CRUTCHER LLP
Palo Alto, CA

HOWREY SIMON ARNOLD & WHITE, LLP
Menlo Park, CA

KEKER & VAN NEST LLP
San Francisco, CA

KIRKLAND & ELLIS
Los Angeles, CA

MAYER, BROWN, ROWE & MAW
Palo Alto, CA

MCDERMOTT, WILL & EMERY
Menlo Park, CA

O'MELVENY & MYERS LLP
San Francisco, CA

ORRICK, HERRINGTON & SUTCLIFFE LLP
San Francisco, CA

PILLSBURY WINTHROP LLP
San Francisco, CA

SHEARMAN & STERLING
San Francisco, CA

TOWNSEND AND TOWNSEND AND CREW LLP
San Francisco, CA

WILSON SONSINI GOODRICH & ROSATI
Palo Alto, CA

Patrons ($5,000 to $9,999)

FISH & NEAVE
Palo Alto, CA

KENYON & KENYON
San Jose, CA

KNOBBE MARTENS OLSON & BEAR LLP
Newport Beach, CA

MANATT, PHELPS & PHILLIPS, LLP
Palo Alto, CA

Comment Competition Prize Sponsor

COOLEY GODWARD LLP
San Francisco, CA

The *Berkeley Technology Law Journal* is a nonprofit organization and welcomes donations. Donors are recognized appropriately for their contributions. For more information, contact the Development Editor, *Berkeley Technology Law Journal*, 587 Simon Hall, Boalt Hall School of Law, University of California, Berkeley, California 94720, (510) 643-6454, or e-mail btlj@law.berkeley.edu.

ADVISORY BOARD

SUBSCRIBER INFORMATION

The *Berkeley Technology Law Journal* (ISSN 1086-3818), a continuation of the *High Technology Law Journal* effective Volume 11, is edited and published four times each year (Spring, Summer, Fall, and Annual Review of Law and Technology) by the students of Boalt Hall School of Law, University of California, Berkeley.

Correspondence. Address all correspondence regarding subscriptions, address changes, claims for nonreceipt, single copies, advertising, and permission to reprint to Kira Abrams, Journal Publications Coordinator, 421 North Addition, Boalt Hall School of Law, Berkeley, California 94720-7200; (510) 643-6600. Authors: see section entitled Information for Authors.

Subscriptions. Annual subscriptions are $65.00 for individuals, and $85.00 for organizations. Single issues are $27.00. Please allow two months for receipt of the first issue. Payment may be made by check, international money order, or credit card (MasterCard/Visa). Domestic claims for nonreceipt of issues should be made within 90 days of the month of publication; overseas claims should be made within 180 days. Thereafter, the regular back issue rate ($27.00) will be charged for replacement. Overseas delivery is not guaranteed.

Form. The text and citations in the *Journal* conform generally to the UNITED STATES GOVERNMENT PRINTING OFFICE STYLE MANUAL (28th ed. 1984) and to THE BLUEBOOK: A UNIFORM SYSTEM OF CITATION (Columbia Law Review Ass'n et al. eds., 17th ed. 2000). Please cite this issue of the *Berkeley Technology Law Journal* as 18 BERKELEY TECH. L.J. ___ (2003).

Postmaster: Send address changes to the *Berkeley Technology Law Journal*, University of California, Berkeley, Boalt Hall School of Law, 587 Simon Hall, Berkeley, California 94720-7200.

BTLJ ONLINE

Abstracts of all *Berkeley Technology Law Journal* and *High Technology Law Journal* articles as well as the full text of most articles published in previous issues can be found at http://www.law.berkeley.edu/journals/btlj. Our site also contains subject, author and title indexes, general information about the *Journal*, selected materials related to technology law, and links to other related home pages. Subject, author and title indexes may also be found in Volume 10, Number 2 (1995) of the *Journal*.

INFORMATION FOR AUTHORS

The Editorial Board of the *Berkeley Technology Law Journal* invites the submission of unsolicited manuscripts. Submissions may include previously unpublished articles, essays, book reviews, case notes, or comments concerning any aspect of the relationship between technology and the law. If any portion of a manuscript has been previously published, the author should so indicate.

Format. Authors should submit double-spaced, single-sided manuscripts with generous margins. We regret that submissions cannot be returned. Authors should retain an exact copy of any material submitted. Authors may submit manuscripts in electronic or hardcopy form, though electronic submissions are strongly encouraged. Electronic submissions should be sent as attachments in Microsoft Word format to btlj@law.berkeley.edu.

Citations. All citations should conform to THE BLUEBOOK: A UNIFORM SYSTEM OF CITATION (Columbia Law Review Ass'n et al. eds., 17th ed. 2000). In addition, the author should include his or her credentials, including full name, degrees earned, academic or professional affiliations, and citations to all previously published legal articles.

Copyrighted Material. If a manuscript contains any copyrighted table, chart, graph, illustration, photograph, or more than eight lines of text, the author must obtain written permission from the copyright holder for use of the material. A photocopy of such written permission should accompany the submission.

Mailing Address. Please submit all hardcopy manuscripts to:

Submissions Editor
Berkeley Technology Law Journal
University of California, Berkeley
Boalt Hall School of Law
587 Simon Hall
Berkeley, California 94720
(510) 643-6454 (Phone)

BOARD OF EDITORS 2002-2003

MEMBERSHIP 2002-2003

Associate Editors

ERIKA ASHMORE
SEÁN PATRICK BUTLER
ALEX EATON-SALNERS
RAECHEL GROOM
SPENCER JACKSON
CHERYL KAHN
ALICE KAO
NICK MARTINI
ELIZABETH MILES
SVETLANA VAS
JENNIFER WAHLSTEN
EMILY WOHL

Members

DAVID ALBAN
JENNIFER BRETAN
STEPHEN BURDICK
LARISSA BURFORD
AARON BURSTEIN
MICHELLE CAI
HENRY CARBAJAL
BENJAMIN CHAPMAN*
CHRISTIN CRAWFORD
JEFFREY DANLEY
KAREN FESSLER
RIP FINST
CHANDRA GARRY
BRIAN GEARING
JESSICA HACKMAN*
DANIEL HIGGS
CODY HOESLY
TERESA HUANG
STEVEN KAM
JENNIE KIM
AMANDA KORNFELD
KARIMAH LAMAR
MICHELLE LAVOIE
JAE HONG LEE
DEZHAN LI
XIAOYU LIN
LIWEN MAH
JOE MARRA
GREGORY NOVOTNY
JOOYOUN PARK
NEIL RANU
RICHARD RONALD
VISHAL SAHNI
SUNAINA SHARMA
MARC SHARP*
MONALI SHETH
ALBERT SIEBER
SHERWIN SIY
CHELSEA TANAKA-DELGADO
KASRA TORABI
JOSEPH TELTSER
CHRISTINA TSOU
EVERT UY
BRYAN WAHL
RUOYU ROY WANG
R. J. KATE WILLIAMS
FELIX WU
P. YVONNE YING
ARMEN ZOHRABIAN

* Denotes Recipient of Outstanding Member Award

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.

EDITED TRANSCRIPT OF THE DAVID NELSON MEMORIAL KEYNOTE ADDRESS: A VOICE FROM CONGRESS ON DRM

By Rep. Zoe Lofgren (D-California)

It's an honor to be here to deliver the David Nelson memorial address. I'd like to thank Pam Samuelson for her gracious invitation to be here today and for her help and expert input on so many of the topics that face us as a nation. I see a lot of friends here this morning too so thank you for being here. As we all know a massive digital media revolution is really unfolding before our eyes. From MP3 players to P2P networks, from digital televisions to personal video recorders, like ReplayTV and TiVo, from e-books to web casting, digital media is changing the way we listen to and view our favorite movies, songs, and books. And like most technological breakthroughs in the past, from the player piano to the VCR, the revolution has aroused deep emotions within the so-called content community. While Jack Valenti has sometimes borne the brunt of unkind comments in the technology community, Jack is someone whom I actually like very much, and who I respect even though I do not always agree with him. I want to read you a quote from Jack, which he has since admitted was incorrect, but if you substitute digital technology for VCR in the quote, it could have been made yesterday. It actually dates back to 1982. Quote: "I say to you that the VCR is to the American film producer and the American public as the Boston strangler is to the woman home alone. . . . . We are going to bleed and bleed and hemorrhage, unless this Congress at least protect[s] one industry that is able to retrieve a surplus balance of trade and whose total future depends on its protection from the savagery and ravages of this machine."

The content industry is actually singing the same tune today. Networks are worried that people will automatically skip commercials with personal video recorders. The studios and the music labels are worried that people will take perfect digital copies of their movies and songs instead of going to the movies or buying CDs.

A few years ago, Congress enacted the Digital Millennium Copyright Act to address their concerns. In return, content owners were supposed to embrace digital technology. Now, almost five years later, content owners are just starting to experiment with new business models that include digital distribution. In my opinion, their progress has been very slow and is at the very least a contributing factor to the huge piracy problem that we face

today. But what's even more troubling is that while content owners have failed to deliver on their promise to embrace digital distribution, the DMCA has also had a number of adverse affects on consumers and entrepreneurs.

As I was thinking about what to say this morning, I took a trip down memory lane. I have been on the House Judiciary Committee for eight years and I've been a member of the Intellectual Property Subcommittee for six. I do believe that protection of intellectual property is important. Copyrights and patents deserve respect, but I also know that intellectual property isn't like Whiteacre and Blackacre and, in fact, you really need to go back to the Constitution to look at what it is we're protecting. In Article 1, Section 8, Congress is asked to secure, for limited times, an author's exclusive right to their work in order to promote the progress of science and useful arts. So this is not a permanent Whiteacre-Blackacre fee simple ownership. It is part of a deal between society and inventors and artists not only to stimulate creativity and innovation, but also [to] use that as a basis for the advancement of science and culture. There are problems with the DMCA relating to fair use and other noninfringing uses that I don't think any of us really had in mind when we drafted the bill. The DMCA, I think, cedes too much power to copyright owners who have no limits on what technical restrictions they put on content. For example, online publishers don't just set the price of digital books, they can control where consumers read books, and the amount of time consumers have to read books. They can even prevent a consumer from sharing their copy with a friend or a family member. Publishers never had this power before. If I buy a book at Barnes and Noble, which I do a lot, a publisher can't control what I do with my copy. I can read it over and over, I can lend it to my son, I can read it at home, on a plane, [and] on vacation.

Copyright holders must recognize that my expectations don't change just because I choose to purchase their product in another format. Another example occurred last year when music fans were shocked to learn that they couldn't play some of their store-bought CDs on their computers. The new CDs even made some Mac computers lock up completely. At the same time, consumers are prevented from circumventing restrictions for any reason, including fair use. It is unlawful to disseminate information about how to evade an encryption, punishable by up to five years in prison and a $500,000 fine.

So what is fair use? It's an important safeguard that's been recognized, as you know, by statute and by the United States Supreme Court, that tries to balance the competing interests of copyright holders in protecting their works, and the public, which needs to have access to information and to be

able to share ideas and to innovate. Really it's what the Framers envisioned when they asked Congress to find that balance. Traditionally, copyright law never gave total control to copyright owners, [whereas] digital rights management, backed by Section 1201 of the DMCA, potentially gives them that power.

[Content holders] can now put a lock . . . on content and restrict fair use and other noninfringing uses, and the public can't do anything about it because it's a crime. I don't think the authors of the DMCA really intended to create such a dramatic shift in the balance. The House Judiciary report accompanying the DMCA stated, and I quote: "an individual should not be able to circumvent in order to gain unauthorized access to a work," but here's the important part, "but should be able to do so in order to make fair use of work that he or she has acquired lawfully." That's what members of Congress thought they were voting to do, however we went much further. We've destroyed the first-sale doctrine. The current system has the potential to destroy, and actually has already destroyed, the first-sale doctrine. It also has the potential of extending copyright in perpetuity. I had the privilege of watching Larry Lessig argue the *Eldred* case before the Supreme Court. I was really intrigued to watch it and I noticed that Larry was very disappointed in the results, and it may seem strange for a member of Congress, but I thought the result was bizarre. If we can't regulate guns in junior high schools based on the implied limitations of the Commerce Clause, the *Eldred* case really makes no sense whatsoever. In any case the point is that given Section 1201 of the Act, even though material is in the public and no longer protected under copyright, [through] technological means, one can, in effect, control content forever, and that is something that I think we really must address.

We've also dampened technological development and competition through the DMCA, and I know that this was not something that we really had in mind. I come from Silicon Valley, I represent Silicon Valley, and every week I come home, and every week I try to visit a new company, usually start-ups or small guys, to see what they are doing. Some of the people I've visited in the past are now running into big problems with the DMCA, like Sonicblue, which created Replay TV. Twenty percent of their quarterly spending is now on litigation. They're trying to lead in innovation but they get sued at every turn. DMCA is chilling competition. Take the case of Lexmark, and this is something I know none of us had in mind. Lexmark-brand printers now have a cryptographic handshake so that the printer can recognize the cartridge. A company called Static Control figured out how to defeat the handshake and build a competing cartridge that worked with Lexmark printers. Lexmark sued under 1201 of the DMCA,

claiming that the handshake is a technological measure that effectively controls access to Lexmark's printer software, [even though] there is no content that is being protected by the handshake.

Now some would say in Washington, "Not a problem because the case is yet to be resolved," but the point is that in Silicon Valley, and in the world at large, it's hard to get venture capital if you're going to spend half of your venture loan on litigation. People are afraid to proceed on innovative measures. I recently met with a company in my district that is working on some technologies to stream digital video from the desktop to the flat panel [television] on the wall. Pretty soon even those of us who aren't rich are going to be able to buy a flat panel and hang it on the wall. I think that'll be really cool, except it's not going to work if we can't get the signals to the flat panel. They've had to stop their technology because it violates the DMCA. And the question is: Why would we do that to ourselves and to society?

In addition to the DMCA chilling innovations, there are other things that are being chilled. Recently I met with another constituent who no longer is pursuing technology to screen songs over cell phones because of the difficulties and the litigations that would result. In addition to the technology innovations that are being chilled, I think there are some other things that are just going to tick off consumers. I gave this to John Conyers on the floor on Thursday: Dateline Detroit, February 24th. WDET 101.9 FM—it's Detroit public radio—they have had to suspend streaming their music program from their website because the RIAA says it violates the DMCA. The RIAA has established these rules: the station is not allowed to play more than two songs in a row by the same artist, not allowed to play more than four songs by the same artist within a three hour period, and so WDET has just stopped streaming their show. Now how does that help advance the course of culture. John Conyers read this on the floor while we were busily making it a felony for scientists to conduct somatic cell nuclear transfer research, and [he] said, "My God, that's my town." Yes indeed. We need to address these issues. And I think a small reflection on how the DMCA was enacted may help us understand the challenges that we face in making the changes.

I was sworn into Congress in January of 1995. As you recall that was the famous moment when Dick Gephardt handed the gavel to Newt Gingrich and it was "Contract with America" time. Shut down the government. It was chaos, the revolutionaries were going to change the world, and so we didn't have time for something as mundane as copyright in the 104th Congress. But by the 105th Congress, there was great concern on the part of very large interests. I mean the movie business, the recording

industries. They were at risk because of the digital revolution and they helped put together the outlines of the DMCA. Now I met with a brand new member of the Intellectual Property Subcommittee and I looked at the bill and I saw some problems, but the bigger problem in retrospect that I see was, on the committee, I was the tech expert. I mean we're in trouble when that occurs. I'm a lawyer, not a techie. I like to play with technology and try to understand it, so I did at least understand that one of the first drafts outlawed web browsers; and I remember calling John Place, who was then general counsel of Yahoo!, who I had met, and I said, "John you need to pay attention to this bill because it outlaws web browsing, and I think that would have an impact on Yahoo!." But they were busy. When I was elected, Jerry Yang was still in a dorm room at Stanford, Marc Andreessen was in the Midwest; these people were building companies rapidly, they were on the cutting edge of technology. They were young and they didn't know Washington and they didn't think what Washington did really would matter to them.

So in the end, we did sort out the web browser problem, but we didn't have any counterforce against the Hollywood people, the RIAA people, and the publishers. And you have to understand that these industry groups have established ties over decades. They are known, they are friendly, they are great lobbyists, and so we ended up with some real problems. I remember Rick Boucher, who was the senior member of the Subcommittee, offering an amendment that indicated that Section 1201 would not apply if the intent was to pursue a noninfringing use. That amendment got two votes: me and Rick. So this is the situation that we find in Washington today. Fortunately, some in the tech world now—after Yahoo went through that experience and realized that most companies wouldn't have a member of the Committee call them four or five times to tell them that they need to pay attention—have hired people to represent their interests; and so now you do have more debate. I'm hopeful that the bill that I introduced last Congress, and I will introduce again next week, could be a vehicle for correcting some of the problems in the DMCA. I think that the bill would ensure that consumers would be able to buy content that is compatible across platforms, [which] would encourage technological development and competition. Specifically, it would allow consumers to make backup copies and to play digital works on preferred digital media devices. It also maintains the first-sale doctrine in the digital age, allowing consumers to sell, in a legal way, their copy of digital works just like they can in the analog world. It also protects fair use rights, and other noninfringing rights, in a world where technology gives copyrighters the power to control all downstream uses of content. Under my bill, consumers would be allowed to cir-

cumvent technical restrictions if those restrictions impeded their rights to make noninfringing use of what they lawfully obtained, and they are given no other choice. In that vein, unlike other proposals, my bill would provide flexibility for content owners to protect their content so long as they enable users to make legitimate uses of the content that they obtained. I believe that, contrary to the claims of some in Washington, this bill does not destroy the DMCA. It would still be illegal to circumvent, or to gain unauthorized access to illegally distribute content. It provides a defense to consumers and I don't think the content industry should be afraid of it.

A Norwegian court recently said in its DeCSS ruling, you shouldn't be prohibited from breaking into your own property. Copyright holders would argue that a consumer hasn't bought any property, but I think they are missing the point. The . . . access to content they're concerned about, is not breaking encryption on the CD that you purchased, it's creating a million CDs in Brazil and selling them, and that is something that I think is legitimately a concern. I'm not hostile to the need to provide financial incentives to those who create content. I think that is very important; but I also equally believe that we need to respect the rights over not just the property, but the rights of the consuming public and really the culture to have information flow. Finally, I think we should understand that this is a battle that is not limited to the United States. Recently, I read in Tech Daily that Mr. Zoellick, our trade negotiator, has made a trade deal with Australia, contingent on their adoption of our version of the DMCA. So we need to be very alert to make sure that that is opposed, and that we get our Congress to listen up and correct the defects in the Digital Millennium Copyright Act. I think this conference is part of doing that. Thank you for being part of it, and I look forward to hearing more. Thank you very much.

THE DMCA AND THE REGULATION OF SCIENTIFIC RESEARCH

By Joseph P. Liu†

ABSTRACT

This Article analyzes the impact of the Digital Millennium Copyright Act (DMCA) on academic encryption research. In this Article, I argue that for both legal and practical reasons academic encryption researchers should be able to conduct and publish certain types of research without significant fear of liability under the DMCA. However, the DMCA will have a non-trivial impact on the conditions under which such research takes place, and this impact can be expected to have several undesirable effects. More broadly, this impact highlights the problematic way in which the DMCA regulates scientific research in furtherance of intellectual property rights. The Article concludes with a number of suggestions for mitigating some of these negative effects.

TABLE OF CONTENTS

---

† Assistant Professor, Boston College Law School. Thanks to Hal Abelson, Stacey Dogan, Dean Hashimoto, Andrew "bunnie" Huang, Pamela Samuelson, Lee Tien, Fred Yen, and the participants at the Second Annual Intellectual Property Scholars Conference at Cardozo Law School, for helpful comments and suggestions. Thanks also to Anderson Kizzie for research assistance. I should disclose at the outset that I have worked with the Electronic Frontier Foundation (EFF) on a number of cases involving the application of the DMCA to encryption research. *See, e.g.*, Compl. Declaratory J. and Injunctive Relief, Felten v. Recording Indus. Ass'n (RIAA) (D.N.J. Nov. 28, 2001) (No. CV-01-2669), *available at* http://www.eff.org/Legal/Cases/Felten_v_RIAA/20010606_eff_felten_complaint.html. The views expressed in this Article, however, are solely mine and do not represent the views of the EFF or any other organization.

I. INTRODUCTION

The Digital Millennium Copyright Act of 1998 (DMCA)[1] has been the subject of significant controversy. In particular, the anti-circumvention provisions of the DMCA[2]—the provisions that impose liability for circumventing technological measures used to protect copyrighted works—have been the target of much criticism from academics, consumer groups, and civil libertarians.[3] DMCA critics have argued that these provisions unduly shift the preexisting balance of interests in copyright law toward copyright holders and away from copyright consumers and the public at large.[4] At the same time, supporters of the DMCA, including members of the movie and music industries, have vigorously defended these provisions, arguing that they are necessary to prevent unauthorized copying of copyrighted works in the digital environment.[5]

My purpose in this Article is not to address, at least directly, the broader debate over the wisdom or propriety of the DMCA's anti-circumvention provisions. Instead, this Article focuses on a much narrower issue: the impact of the DMCA on academic encryption research. For the purpose of this Article, let us assume that the basic objective of the anti-circumvention provisions—the desire to help copyright owners use technology to protect their works—is a good one, or at least unobjectionable. In pursuing this objective, what impact does the DMCA, as currently drafted, have on the ability of academic encryption researchers to pursue

---

1. Digital Millennium Copyright Act, 17 U.S.C. §§ 101-1205 (2000).

2. *Id.* § 1201.

3. The DMCA contains several additional provisions, unrelated to the anti-circumvention provisions that are the subject of this Article. *See, e.g.*, *Id.* § 512. For purposes of saving space, any mention of the DMCA in this Article references the anti-circumvention provisions.

4. *See, e.g.*, JESSICA LITMAN, DIGITAL COPYRIGHT (2001); Glynn S. Lunney, Jr., *The Death of Copyright: Digital Technology, Private Copying, and the Digital Millennium Copyright Act*, 87 VA. L. REV. 813 (2001); *cf.* Pamela Samuelson, *Intellectual Property and the Digital Economy: Why the Anti-Circumvention Regulations Need to be Revised*, 14 BERKELEY TECH. L.J. 519 (1999).

5. *See, e.g., WIPO Copyright Treaties Implementation Act: Hearings on H.R. 2281 Before the House Comm. on Commerce Subcomm. on Telecommunications, Trade and Consumer Prot. House Commerce Comm.*, 104th Cong. (1998) [hereinafter *Hearings on H.R. 2281*] (statements of Steven J. Metalitz representing the Motion Picture Association of America and Robert W. Holleyman, II of the Business Software Alliance), *available at* http://www.ipmall.info/hosted_resources/June5-98Hearing.pdf (last visited May 4, 2003); *cf.* David Nimmer, *Appreciating Legislative History: The Sweet and Sour Spots of the DMCA's Commentary*, 23 CARDOZO L. REV. 909, 927 (2002) (noting that "the DMCA enjoys widespread support from the motion picture, recording, software, and publishing industries").

their scientific research? And how should we evaluate this impact, as a normative matter?

Recently, there has been some debate over the extent to which academic encryption researchers should reasonably fear liability under the DMCA for certain forms of research. Although the DMCA contains an express exemption for encryption research,[6] many encryption researchers have argued that the exemption is too narrow to be of practical use.[7] Moreover, a number of recent cases have spurred fears among researchers that, despite the exemption, they may be liable for activities they routinely undertake in the course of their research.[8] Other commentators, however, have argued that these fears are unwarranted under a proper reading of the statute, and that such fears may be exaggerated by DMCA critics to increase opposition to the DMCA.[9]

In this Article, I argue that, under certain circumstances, academic encryption researchers can continue to conduct and publish certain types of research without much practical risk of DMCA liability. This conclusion rests in part on a close reading of the statute and on predictions about how courts will likely interpret these statutory provisions in the context of academic encryption research. This conclusion also rests in part on an assessment of practical considerations surrounding DMCA litigation, such as the negative publicity such lawsuits tend to engender in light of recent, prominent cases. Thus, practically speaking, certain types of academic encryption research can still occur under the DMCA.

However, the DMCA *does* have a non-trivial impact on the conditions under which such research takes place. Specifically, the DMCA: imposes additional hurdles, which researchers must overcome before engaging in and publishing their research; limits the universe of individuals with whom researchers can freely communicate about their research; requires disclosure of the intention to engage in research and the fruits of such research to third-parties; affects the content of academic research papers; and limits avenues for publication of the research. Thus, even though academic encryption researchers can continue to conduct and publish some of their research under the DMCA without significant practical risk of criminal or civil liability, the DMCA significantly affects the manner in which that research is conducted.

---

6. *See* 17 U.S.C. § 1201(g).

7. *See infra* Part II.B.

8. *See infra* Part II.C.

9. *See, e.g.*, Declan McCullagh, *Debunking DMCA Myths*, CNET NEWS.COM (Aug. 19, 2002), *at* http://news.com.com/2010-12-950229.html [hereinafter McCullagh, *Debunking DMCA Myths*].

Are these additional burdens on encryption research justified? In this Article, I will argue that they are not. I will argue that we should be extremely hesitant to impose any burdens on the conduct of basic scientific research in order to further an interest in the protection of intellectual property rights. Indeed, the DMCA represents a rather radical attempt by Congress to regulate not just copyright infringement or even the tools that facilitate infringement, but the basic research that could potentially be used to create tools that facilitate infringement. By imposing even minimal burdens on activity that is so far upstream from the actual infringing activity, we risk affecting many collateral areas of technology that are unrelated to the purported harm of copyright infringement.

From these conclusions, I argue that academic encryption researchers should have the widest possible freedom to conduct, discuss, and disseminate their research. Rather than placing any conditions on the research itself, the DMCA should focus on regulating concrete and problematic applications of the fruits of such scientific research. Any regulation of encryption research should be narrowly limited to distinguishing such research from activities that are clearly intended to facilitate infringement. The DMCA's encryption research exemption purports to do this, but in fact does much more. This recommendation could be implemented through proposed amendments to the DMCA or, alternatively, through expansive judicial interpretations of the encryption research exemption.

Although the topic of this Article is narrow, it is an important one. Encryption is a vital component of our current communications infrastructure.[10] Anything that affects the ability of scientists to study and improve encryption technology therefore deserves careful scrutiny. More broadly, a close look at the DMCA's impact on encryption research can generate useful insights into the DMCA's overall regulatory approach. This Article focuses specifically on academic encryption researchers because nearly everyone agrees that the DMCA should leave their activities largely unaffected.[11] By studying whether the DMCA in fact successfully does so, this Article can shed some interesting light on how we should think about intellectual property protection and its collateral effects on scientific research.

---

10. *See, e.g.*, Michael Froomkin, *The Metaphor is the Key: Cryptography, the Clipper Chip and the Constitution*, 143 U. PENN. L. REV. 709 (1995).

11. The distinction between "academic" and "nonacademic" encryption researchers is developed more fully *infra* in Parts III.B and IV.

II. BACKGROUND ON THE DMCA AND ENCRYPTION RESEARCH

A. The DMCA and the Encryption Research Exemption

In 1998, Congress passed the DMCA in response to perceived challenges presented by digital and network technologies.[12] The DMCA lends additional legal support to copyright owners' efforts to protect their works using technology. It does so by imposing liability on individuals who circumvent access control technologies, such as encryption.[13] It also imposes liability for the dissemination of devices or technologies that are primarily designed for the purpose of, or have few commercially viable uses other than, facilitating such circumvention.[14] Finally, the DMCA contains provisions that impose liability for removing or altering "copyright management information" attached to copyrighted files.[15]

When the bill that eventually became the DMCA was first introduced, it contained no exemption for encryption research. This was partly because Congress believed that the DMCA would rarely interfere with encryption research, since it thought that such research would not typically involve circumventing protection mechanisms actually deployed in commerce.[16] However, members of the encryption research community testified at hearings, expressing concern that the DMCA would hinder their efforts, since much valuable research is performed on systems as they are actually deployed in the field.[17] Indeed, this kind of real-world testing is the only way to find out whether an encryption system is secure.

---

12. I will begin here with a brief background on the DMCA and the encryption research exemption. Those already familiar with this material may wish to skip to the next section. I focus here primarily on the legal background. For general background on cryptography and encryption research, see Brief of Amici Curiae Dr. Steven Bellovin et al., Universal City Studios, Inc. v. Corley, 273 F.3d 429 (2d Cir. 2001) (No. 00-9185) [hereinafter Cryptographers' Brief], *available at* http://cyber.law.harvard.edu/openlaw/DVD/NY/appeals/010126-cryptographers-amicus.pdf (last visited May 5, 2003) and BRUCE SCHNEIER, APPLIED CRYPTOGRAPHY (2d ed. 1996).

13. 17 U.S.C. § 1201(a)(1) (2000).

14. *See id.* §§ 1201(a)(2), 1201(b).

15. *Id.* § 1202.

16. *See* S. REP. NO. 105-190, 1998 WL 239623, at *15-16 (1998).

17. *See, e.g.*, *Hearings on H.R. 2281, supra* note 5, at 4-6. Jonathan Callas testified:

> In order to ensure that a cryptographic system has no weaknesses, either in the cryptography itself or in its application and implementation, it is essential that we continually attempt to break that system.
>
> . . . .

As a result of this testimony, the final version of the DMCA contained an express exemption for encryption research.[18] The exemption shields encryption researchers from liability for circumventing access-control technologies under certain circumstances.[19] The exemption defines "en-

---

> It is essential to test technology as it is applied—i.e. when it is being used to protect something, because most weaknesses in cryptography occur in its application.

Id. (emphasis original), *available at* http://www.ipmall.info/hosted_resources/June5-98 Hearing.pdf (last visited May 4, 2003); *see also* Cryptographers' Brief, *supra* note 12, at 29-30, *available at* http://cyber.law.harvard.edu/openlaw/DVD/NY/appeals/010126-cryptographers-amicus.pdf ("The advancement of the science of cryptography depends on researchers' ability to study signals 'in the wild,' not only those codes developed for academic purposes, since the implementation may be as important as the algorithm in determining a system's security.").

18. It is worth noting that the European Union Directive and certain implementations of the WIPO treaties regarding anti-circumvention legislation contain no exemption for encryption research.

19. 17 U.S.C. § 1201(g) states:

> Encryption research.
>
> (1) Definitions. For purposes of this subsection—
>
> (A) the term "encryption research" means activities necessary to identify and analyze flaws and vulnerabilities of encryption technologies applied to copyrighted works, if these activities are conducted to advance the state of knowledge in the field of encryption technology or to assist in the development of encryption products; and
>
> (B) the term "encryption technology" means the scrambling and descrambling of information using mathematical formulas or algorithms.
>
> (2) Permissible acts of encryption research. Notwithstanding the provisions of subsection (a)(1)(A), it is not a violation of that subsection for a person to circumvent a technological measure as applied to a copy . . . of a published work in the course of an act of good faith encryption research if—
>
> (A) the person lawfully obtained the encrypted copy . . . ;
>
> (B) such act is necessary to conduct such encryption research;
>
> (C) the person made a good faith effort to obtain authorization before the circumvention; and
>
> (D) such act does not constitute infringement under this title or a violation of applicable law other than this section . . . .
>
> (3) Factors in determining exemption. In determining whether a person qualifies for the exemption under paragraph (2), the factors to be considered shall include—
>
> (A) whether the information derived from the encryption research was disseminated, and if so, whether it was disseminated in a manner reasonably calculated to advance the state of knowledge or development of encryption technology, versus whether it was disseminated in a manner that facilitates infringement . . .

cryption research" as "activities necessary to identify and analyze flaws and vulnerabilities of encryption technologies applied to copyrighted works, if these activities are conducted to advance the state of knowledge in the field of encryption technology or to assist in the development of encryption products."[20] Encryption research is exempt from liability for circumvention if it is conducted in "good faith," provided that the encrypted copy is lawfully obtained, the act of circumvention is "necessary" for the research, and the researcher made a good faith effort to obtain authorization from the copyright owner before engaging in the circumvention.[21]

In determining whether the exemption applies, Congress directed courts to consider a number of factors,[22] including the manner in which information derived from the research is disseminated and whether the researcher "is engaged in a legitimate course of study, employed, or is appropriately trained or experienced, in the field of encryption technol-

---

> (B) whether the person is engaged in a legitimate course of study, is employed, or is appropriately trained or experienced, in the field of encryption technology; and
> (C) whether the person provides the copyright owner of the work to which the technological measure is applied with notice of the findings and documentation of the research, and the time when such notice is provided.
> (4) Use of technological means for research activities. Notwithstanding the provisions of subsection (a)(2), it is not a violation of that subsection for a person to—
> (A) develop and employ technological means to circumvent a technological measure for the sole purpose of that person performing the acts of good faith encryption research described in paragraph (2); and
> (B) provide the technological means to another person with whom he or she is working collaboratively for the purpose of conducting the acts of good faith encryption research described in paragraph (2) or for the purpose of having that other person verify his or her acts of good faith encryption research described in paragraph (2).

Id.

20. *Id.* § 1201(g)(1)(A).

21. *Id.* § 1201(g)(2)(A)-(C).

22. The precise role played by the factors in § 1201(g)(3) is not entirely clear from the text of the statute. The specific requirements for the exemption are listed in § 1201(g)(2), and one would expect that satisfaction of these requirements would be sufficient for the exemption to apply. However, § 1201(g)(3) goes on to list additional "factors," which a court should consider in determining whether an individual "qualifies for" the exemption. This suggests that these additional factors play some role, although it is not clear precisely what role, since § 1201(g)(2) appears self-contained and does not seem to contemplate consideration of these additional factors. One way of perhaps understanding these additional factors is as a gloss on the general "good faith" requirement in § 1201(g)(2).

ogy."[23] The DMCA further permits researchers to develop the tools necessary to engage in such research and to share such tools with "another person with whom he or she is working collaboratively for the purpose of conducting the acts of good faith encryption research."[24] This last provision shields the researcher from liability under the "tools" provision of the DMCA.[25] Finally, the exemption directs the Register of Copyrights to study the impact of the DMCA on encryption research and to report back to Congress within one year of enactment.[26]

The exemption was essentially an attempt by Congress to preserve some freedom for encryption research while ensuring that the exemption would not create a loophole for illegitimate attempts to exploit vulnerabilities under the cover of encryption research.[27] The House Commerce Report recognized that the DMCA, as originally drafted, had the potential to stifle encryption research and thereby cause substantial harm. Moreover, after hearing testimony by encryption researchers, the House Commerce Committee believed that encryption researchers needed the ability to test encryption technologies not just under laboratory conditions, but also as they are applied in the real world.[28] The exemption was thus an attempt to

---

23. 17 U.S.C. § 1201(g)(3)(A)-(C).

24. *Id.* § 1201(g)(4)(A)-(B).

25. *Id.* § 1201(a)(2).

26. *See id.* § 1201(g)(5).

27. *See* H.R. REP. NO. 105-511 (II), 1998 WL 414916, at *26-27, *43-44 (1998) [hereinafter House Commerce Report 511].

28. *Id*. at *27. The Report states:

> The effectiveness of technological protection measures to prevent theft of works depends, in large part, on the rapid and dynamic development of better technologies, including encryption-based technological protection measures. The development of encryption sciences requires, in part, ongoing research and testing activities by scientists of existing encryption methods, in order to build on those advances, thus promoting and advancing encryption technology generally. This testing could involve attempts to circumvent or defeat encryption systems for the purpose of detecting flaws and learning how to develop more impregnable systems. The goals of this legislation would be poorly served if these provisions had the undesirable and unintended consequence of chilling legitimate research activities in the area of encryption.
>
> In many cases, flaws in cryptography occur when an encryption system is actually applied. Research of such programs as applied is important both for the advancement of the field of encryption and for consumer protection. Electronic commerce will flourish only if legitimate encryption researchers discover, and correct, the flaws in encryption systems before illegitimate hackers discover and exploit these flaws. Accord-

strike a balance and to sort out "legitimate" encryption research from "illegitimate" hacking that would lead to increased piracy.[29]

B. Criticism of the DMCA and the Exemption

Since passage of the DMCA, many legal and scientific commentators have criticized the exemption for being both too narrow and too vague, thereby chilling legitimate scientific encryption research.[30] Commentators have critiqued the exemption on several grounds.[31] First, many commenta-

---

> ingly, the Committee has fashioned an affirmative defense to permit legitimate encryption research.

Id.

29. *Id*. at *44. The Report states:

> The Committee recognizes that courts may be unfamiliar with encryption research and technology, and may have difficulty distinguishing between a legitimate encryption researcher and a so-called 'hacker' who seeks to cloak his activities with this defense. Section 102(g)(3) therefore contains non-exclusive list of factors a court shall consider in determining whether a person properly qualifies for the encryption research defense.

Id.

30. *See, e.g.*, Cryptographers' Brief, *supra* note 12 at 9-10, 27-29, *available at* http://cyber.law.harvard.edu/openlaw/DVD/NY/appeals/010126-cryptographers-amicus.pdf; COMM. ON INTELL. PROP. RIGHTS & EMERGING INFO. INFRASTRUCTURE, NAT'L RESEARCH COUNCIL, THE DIGITAL DILEMMA: INTELLECTUAL PROPERTY IN THE INFORMATION AGE 2 (Nat'l Academy Press, *available at* http://books.nap.edu/books/0309064996/html/2.html/index.html, 2000); Cassandra Imfeld, *Playing Fair With Fair Use? The Digital Millennium Copyright Act's Impact on Encryption Researchers and Academicians*, 8 COMM. L. & POL'Y 111 (2003); Michael Landau, *Has the Digital Millennium Copyright Act Really Created a New Exclusive Right of Access?: Attempting to Reach a Balance Between Users' and Content Providers' Rights*, 49 J. COPYRIGHT SOC'Y U.S.A. 277, 306-09 (2001); Pamela Samuelson, *Anti-Circumvention Rules: Threat to Science*, 293 SCI. 2028 (2001); Pamela Samuelson, *Intellectual Property and the Digital Economy: Why the Anti-Circumvention Regulations Need to be Revised*, 14 BERKELEY TECH. L.J. 519 (1999); Pamela Samuelson & Suzanne Scotchmer, *The Law and Economics of Reverse Engineering*, 111 YALE L.J. 1575, 1647-49 (2002); Brian Bolinger, Comment, *Focusing on Infringement: Why Limitations on Decryption Technology Are Not the Solution to Policing Copyright*, 52 CASE W. RES. L. REV. 1091 (2002); Michael Landau, *The DMCA's Chilling Effect on Encryption Research*, *at* http://www.gigalaw.com/articles/2001-all/landau-2001-09-all.html (last visited May 5, 2003).

31. Many of these objections were expressed in the comments to the Register of Copyrights, which were solicited in fulfillment of the Copyright Office's statutory duty to report, within one year of the DMCA's enactment, on the impact of the DMCA on encryption research. *See* NAT'L TELECOMM. INFO ADMIN. & U.S. COPYRIGHT OFFICE, REPORT TO CONGRESS: JOINT STUDY OF SECTION 1201(G) OF THE DIGITAL MILLENNIUM COPYRIGHT ACT, *at* http://www.copyright.gov/reports/studies; Comments of Jonathan D. Callas, *at* http://www.copyright.gov/reports/studies/comments/012.pdf (July 26, 1999) [hereinafter Callas Comment]; Comments of EMusic.com, Inc., *at* http://www.copyright.-

tors have argued that the definitions of encryption and encryption research are too narrow. In particular, they have taken issue with the requirement that the act of circumvention be "necessary" for the research. The fear is that researchers will be chilled if they feel the need to prove that the act was "necessary," as opposed to being merely important or useful.[32]

Second, commentators have criticized the requirement that a researcher first seek authorization from the copyright owner before engaging in the act of circumvention. They question whether this amounts to a requirement that the copyright owner approve of the circumvention, in which case the exemption will be meaningless.[33] On the other hand, if, as the text of the exemption suggests, all that is required is a request and not approval, then the requirement serves no purpose other than to place the copyright owner on notice, thereby inviting a potential lawsuit or the imposition of burdensome conditions and limitations on dissemination of the research.[34] In either case, the requirement is problematic as it may chill legitimate research.

---

gov/reports/studies/comments/010.pdf (July 26, 1999) [hereinafter EMusic.com Comment]; Comments of the Computer & Communications Indus. Ass'n (CCIA) *at* http://www.copyright.gov/reports/studies/comments/011.pdf (submitted July 26 1999) [hereinafter CCIA Comment]; Comments of Hal Finney, *at* http://www.copyright.gov/reports/studies/comments/003.pdf (July 12, 1999) ("Prudent researchers who do not want to risk criminal prosecution will avoid work in this area . . . . The result will be a loss of confidence in cryptographic technology as users realize that the best and brightest researchers are no longer able to do research in this field. This will harm electronic commerce and damage American interests domestically and internationally.") [hereinafter Finney Comment]; Comments of Kroll O'Gara Information Security Group, *at* http://www.copyright.gov/reports/studies/comments/007.pdf (submitted July 26, 1999) [hereinafter O'Gara Comment]; Comments of David Wagner, *at* http://www.copyright.gov/reports/studies/comments/001.pdf (May 27, 1999) ("As an encryption researcher, I don't think I will be going out on a limb to predict that this law is about to have a negative effect on encryption research . . . .") [hereinafter Wagner Comment]. However, the Register ultimately concluded that these concerns were still hypothetical, they had already been raised when the DMCA was being considered, and there was as yet no concrete evidence, nor were there specific examples, of encryption research being hindered in any way. As the Register recognized, this was not surprising, given that the report was due one year before the anti-circumvention provisions were to go into effect.

32. *See* Finney Comment, *supra* note 31.

33. *Id*. ("Provision (C) can only be described as bizarre. There is no requirement elsewhere in the exemptions to receive authorization from the copyright holder. Apparently, whether authorization is granted or not makes no difference, but nevertheless the researcher is required to seek authorization? This is completely illogical."); *see also* Callas Comment, *supra* note 31.

34. Bolinger, *supra* note 30, at 1097-98 ("Although sharing one's results with the party most affected by them is reasonable given the general policy goal of improving and

Third, commentators have taken issue with the additional factors—particularly the factor that looks to the training or affiliation of the researcher—used to determine whether a researcher "qualifies" under the exemption. This is because encryption research is characterized, somewhat unusually, by the active participation of individuals or "hobbyists" who are not affiliated with a research organization or who may not have had any formal training. Indeed, such individuals commonly play a significant role in testing the security of implemented systems and publicizing weaknesses in such systems.[35]

Fourth, commentators argued that the exemption is ambiguous regarding the extent to which researchers may publish or share their results with others. The exemption itself hints that dissemination of information may be permissible so long as it is done in a manner that is "reasonably calculated to advance the state of knowledge or development of encryption technology."[36] However, the exemption does not state this outright. Moreover, many commentators have argued that the exemption from liability under the tools provision is too narrow.[37] According to these commentators, an essential part of publishing the results of encryption research is providing others with the tools to verify and comment upon the results. Frequently this involves sharing either actual code or descriptions that are sufficiently detailed to enable others to create their own code.[38] These activities could lead to liability under the tools provision. Furthermore, the

---

strengthening encryption techniques, under the present state of the law, such an action is tantamount to an invitation to be sued.").

35. *See* Cryptographers' Brief, *supra* note 12, at 24, *available at* http://cyber.law.harvard.edu/openlaw/DVD/NY/appeals/010126-cryptographers-amicus.pdf ("The exception of 1201(g) endorses a fundamentally mistaken conception of cryptographic science, one in which advances are predictable, generated only from within an 'establishment,' and where limited, strictly regulated testing suffices to assure the security of cryptosystems."); Callas Comment, *supra* note 31 ("An interesting aspect of today's research is that relative unknowns do some of the most important new work.").

36. 17 U.S.C. § 1201(g)(3)(A) (2000).

37. *See, e.g.*, Cryptographers' Brief, *supra* note 12, at 14, *available at* http://cyber.law.harvard.edu/openlaw/DVD/NY/appeals/010126-cryptographers-amicus.pdf. The Brief states:

> The science of cryptography depends on cryptographers' ability to exchange ideas in code, to test and refine those ideas, and to challenge them with their own code. By communicating with other researchers and testing each others' work, cryptographers can improve the technologies they work with, discard those that fail, and gain confidence in technologies that have withstood repeated testing.

Id.

38. *Id.*

exemption is too narrow insofar as it limits such sharing only to collaborators and not to the wider research community.

Fifth, commentators have expressed concern that the exemption is incomplete as it only applies to liability under § 1201(a) for circumventing access-control technologies, but does not apply to liability under § 1201(b) for distribution of devices that circumvent copy-control technologies.[39] Some forms of research might well give rise to liability under both provisions.[40] Nor does the exemption apply to liability under § 1202, which involves the integrity of copyright management information.[41] For example, the provision would not shield from liability a researcher who wished to remove a digital watermark containing copyright management information. Thus, an encryption researcher may be shielded from liability under § 1201(a), but still subject to liability under these alternative provisions.

Finally, commentators have argued that the above flaws would have a chilling effect on encryption research without any offsetting benefit in the form of added security for copyright owners. The testing of implemented systems can still take place in other countries, since the DMCA's impact is largely limited to the United States, and many other countries have no equivalent statute. Moreover, individuals will continue to attack and exploit the weaknesses of such systems anonymously. Given the ease with which one can distribute information about the weaknesses of encryption systems over the Internet, the DMCA will do little to reduce the incidence of circumvention or the availability of circumvention technologies.

Indeed, according to commentators, the DMCA will actually make encryption technologies more susceptible to such attacks, since copyright owners will not be able to improve their systems using the results of open and legitimate encryption research. That is, by chilling legitimate encryption research, the DMCA will simply drive encryption research into less legitimate channels. Weaknesses discovered by attackers will not be published and reviewed in academic journals or on the Internet. Consequently, individuals and companies will never be confident that any proposed or implemented systems are robust and secure.[42]

---

39. *See generally* Bolinger, *supra* note 30, at 1100.

40. *See* R. Anthony Reese, *Legal Incentives for Adopting Digital Rights Management Systems: Merging Access Controls and Rights Controls*, 18 BERKELEY TECH. L.J. 619, 622-27 (2003) (analyzing in detail the ways in which implemented systems may be protected as both access and rights control technologies).

41. 17 U.S.C. § 1202(b).

42. *See* EMusic.com Comment, *supra* note 31. EMusic.com states:

> While there is a superficial appeal to the argument that these security implementations would have had a longer shelf-life had their vulnerabilities *not* been revealed, in the long run, there is greater benefit from

C. Initial Cases Implicating the Exemption

Despite these objections, the anti-circumvention provisions of the DMCA went into effect in October of 2000, and since then a few cases implicating the encryption research exemption have arisen. The first case to consider the encryption research exemption did so only briefly. That case, *Universal City Studios, Inc. v. Reimerdes*,[43] involved a DMCA claim against the publication and distribution of DeCSS, a program that enabled decryption of DVDs. DeCSS was created by a Norwegian programmer, ostensibly to permit individuals to play DVDs on the Linux operating system, and then posted on a website by the defendants. One of the defendants' arguments was that DeCSS represented legitimate encryption research.[44] The court quickly rejected this argument, emphasizing the defendants' failure either to seek permission from or to provide the results of their research to the copyright owners.[45]

The second case involving the exemption occurred in a context better suited to the exemption. *Felten v. RIAA*[46] concerned the activities of a number of academic encryption researchers who cracked a watermarking technology called SDMI, which the recording industry was planning to deploy in order to protect recorded music from being copied. The recording industry had issued a public challenge inviting individuals to try to crack the technology. The plaintiffs were a team of researchers from various institutions, including Princeton and Rice, who took up that challenge and succeeded. When they tried to publish an academic paper detailing their research, they received a threatening letter from the RIAA, which claimed that publication of the paper could result in liability under the DMCA. In response, the researchers withdrew their paper from an academic conference. They later filed suit against the RIAA, seeking a decla-

---

> having those vulnerabilities revealed. This is particularly true when reliance on a particular security implementation could lead to significant industry and consumer investment in hardware and software devices that support that implementation.

Id. at 4 (emphasis original); *see* Finney Comment, *supra* note 31 ("By driving the legitimate experts into other avenues of research, the DMCA will leave the field to those who care nothing about laws. To paraphrase another slogan, if you outlaw cryptographic research, only outlaws will do cryptographic research.").

43. 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).

44. *See id*. at 320-21.

45. *See id*. at 321.

46. Compl. Declaratory J. and Injunctive Relief, *Felten* (No. CV-01-2669), *available at* http://www.eff.org/Legal/Cases/Felten_v_RIAA/20010606_eff_felten_complaint.html.

ration that their activities did not violate the DMCA. After much back-and-forth, the RIAA eventually acceded to the publication of the paper, and the case was dismissed.[47]

The third case was a criminal prosecution against Dmitri Sklyarov, a Russian programmer.[48] Sklyarov had cracked the technological protection measure used by Adobe to control access to copyrighted content distributed in its eBook format. The Russian company he worked for distributed his circumvention software over the Internet. When Sklyarov traveled to the United States to present a paper on his research at a conference, he was arrested and charged with criminal violations of the DMCA. Although Sklyarov eventually reached an agreement with the U.S. government, prosecution continued against Sklyarov's company, Elcomsoft. After trial, the jury acquitted Elcomsoft based on a finding that the corporation did not satisfy the statutory intent requirement for criminal liability.[49]

In addition to the cases above, a number of other incidents implicating the DMCA and encryption research have been reported in the press.[50]

Although all of the cases above implicate, to some extent, the encryption research exemption, none resulted in an opinion comprehensively interpreting the exemption in the context of academic encryption research. Accordingly, uncertainty persists regarding the precise extent to which encryption research is privileged under the DMCA.

D. Responses by Encryption Researchers

The cases above, along with the criticisms of the encryption research exemption, have led to a good deal of concern within the encryption research community. In particular, a number of encryption researchers have refused to publish their research results in response to concerns about

---

47. For additional information about *Felten*, including the court filings, court orders, and other resources, see the Electronic Frontier Foundation's website at http://www.eff.org/IP/DMCA/Felten_v_RIAA/ (last visited Apr. 27, 2003).

48. Compl., United States v. Elcomsoft, 203 F. Supp. 2d 1111 (N.D. Cal. 2002) (No. 5-01-257), *available at* http://www.eff.org/IP/DMCA/US_v_Elcomsoft/20010707_complaint.html (last visited May 5, 2003).

49. For additional information about *Sklyarov*, see the Electronic Frontier Foundation's website at http://www.eff.org/IP/DMCA/US_v_Elcomsoft/ (last visited Apr. 27, 2003).

50. *See, e.g.*, Declan McCullagh, *HP Backs Down on Copyright Warning*, CNET NEWS.COM (Aug. 1, 2002), *at* http://news.com.com/2100-10230947745.html (describing how Hewlett-Packard backed off from initial DMCA threat against researchers for publishing information on flaw in operating system) [hereinafter McCullagh, *HP Backs Down*]; *cf.* David Becker, *MIT Student Hacks into Xbox*, CNET NEWS.COM (June 3, 2002), *at* http://news.com.com/2100-1040-931296.html (describing MIT student publication of paper on security flaws in the Microsoft Xbox).

DMCA liability.[51] For example, the Dutch cryptographer Niels Ferguson declined to publish the results of research he had conducted regarding High Bandwidth Digital Content Protection, a system used by Intel to encrypt video. Ferguson, an independent cryptography consultant, indicated that he had found weaknesses in that system, but decided not to publish the results and removed all references to this research from his website for fear of DMCA liability.[52] Other researchers have similarly indicated that they have withheld or declined to publish their research results out of the same concern.[53]

Professional associations and conferences have also modified their practices in response to the fear of DMCA liability. Some encryption researchers have suggested boycotting encryption research conferences held in the United States.[54] Some conference organizers have decided to hold their conferences outside the U.S., in order to minimize concerns about liability. In addition, in November 2001, the Institute of Electrical and Electronics Engineers (IEEE), a major publisher of computer science journals, began requiring that all authors indemnify the IEEE for DMCA liability resulting from the publication of their research in the journal. The IEEE later withdrew this requirement in response to widespread objections.[55]

---

51. *See generally* Elec. Frontier Found., *Unintended Consequences: Four Years Under the DMCA*, *at* http://www.eff.org/IP/DMCA/20030103_dmca_consequences.pdf (last visited May 4, 2003) [hereinafter Elec. Frontier Found., *Unintended Consequences*].

52. *See* Niels Ferguson, *Censorship in Action: Why I Don't Publish My HDCP Results* ("I have written a paper detailing security weaknesses in the HDCP content protection system. I have decided to censor myself and not publish this paper for fear of prosecution and/or liability under the US DMCA law."), *at* http://www.macfergus.com/niels/dmca (Aug. 15, 2001); *see also* Lisa Bowman, *Researchers Weigh Publication, Prosecution*, CNET NEWS.COM (Aug. 15, 2001), *at* http://news.com.com/2100-1023-271712.html.

53. *See* Robert Lemos, *Security Workers: Copyright Law Stifles*, CNET NEWS.COM (Sept. 6 2001), *at* http://news.cnet.com/2100-1001-272716.html; Wade Roush, *Breaking Microsoft's e-Book Code*, TECH. REV. (Nov. 1, 2001), at 24, *available at* http://www.technologyreview.com/articles/innovation11101.asp. *See generally* Elec. Frontier Found., *Unintended Consequences*, *supra* note 51, at 3-4 (describing how Fred Cohen, a well-respected professor of digital forensics and consultant, and Dug Song, a network security protection expert, removed content from their websites fearing liability).

54. *See* Will Knight, *Computer Scientists Boycott U.S. Over Digital Copyright Law*, NEW SCIENTIST (July 23, 2001), *available at* http://www.newscientist.com/news/news.jsp?id=ns99991063; s*ee also* Elec. Frontier Found., *Unintended Consequences*, *supra* note 51, at 4 (discussing encryption researcher reaction to the arrest of Sklyarov).

55. Will Knight, *Controversial Copyright Clause Abandoned*, NEW SCIENTIST (Apr. 15, 2002), *available at* http://www.newscientist.com/news/news.jsp?id=ns99992169; s*ee also* Elec. Frontier Found., *Unintended Consequences*, *supra* note 51, at 4.

The above responses indicate that many encryption researchers are in fact worried about potential liability. Indeed, some have indicated that they are avoiding research topics that might implicate DMCA liability. As encryption researcher David Wagner put it in his comments submitted to the Register of Copyrights:

> As an academic researcher, I personally find it a little scary to consider doing research on copyright protection schemes, because of 1201(g). I analyze real-world security systems. If, in doing so, I discover a weakness in some deployed system, I face an unsavory choice: tell no one, or publish. If I decide to publish, I have to worry about the threat of retaliation from those trying to sell the flawed system. Whether or not I would eventually win in court, the threat of having to spend time and money on a lawsuit is enough to make me tend to shy away from studying copyright protection.[56]

Despite these claims about the chilling effect of the DMCA on encryption researchers, a number of commentators have recently suggested that such fears of liability are greatly exaggerated and that there is no real risk to academic encryption researchers for the conduct and publication of their research.[57] Pointing to the text of the DMCA, these commentators argue that it would be a significant stretch for a court to find the mere publication of a research paper a violation of the "tools" provision of the DMCA. Moreover, the risk of criminal liability under the DMCA appears to be extremely low, if not non-existent, given past enforcement patterns and government statements regarding criminal liability for research.[58] According to these commentators, encryption researchers should feel comfortable publishing their results.[59] Some commentators have even suggested that DMCA critics have intentionally exaggerated its potential scope in order to increase opposition to the law.[60]

---

56. Wagner Comments, *supra* note 31.

57. *See* McCullagh, *Debunking DMCA Myths*, *supra* note 9, *at* http://news.com.com/2010-12-950229.html.

58. *See id*. ("The risk that a researcher could go to jail for giving a speech at an academic conference is essentially zero.") (quoting George Washington University law professor Orin Kerr).

59. *See id*.

60. *See id*. (quoting Allan Adler of the Association of American Publishers as stating that "[EFF] succeeded in creating a kind of chilling effect in the scientific community because of the kind of fear-mongering they were engaged in.").

III. IMPACT OF THE DMCA ON ENCRYPTION RESEARCH

Are the fears of academic encryption researchers reasonable or exaggerated? More broadly, what impact can we reasonably expect the DMCA to have on academic encryption research? In this part of the Article, I argue that, under certain circumstances, academic encryption researchers can continue to conduct and publish certain types of research without significant fear of legal liability or much practical risk of being sued. At the same time, however, the DMCA has a significant impact on the conditions under which such research is conducted. Although the DMCA does not *prevent* academic encryption research, it does *regulate* it—and it is this more subtle impact of the DMCA that we should be concerned about.

A. Academic Encryption Research Can Still Take Place

In assessing whether encryption researchers face a realistic risk of DMCA liability, the first step is to determine the substantive basis for these concerns. That is, based on a close reading of the statute, legislative history, and limited case law, how likely is it that a court would find an academic encryption researcher liable under the DMCA for conducting and publishing his or her research?[61] To answer this question, it may be useful to look at three separate acts of the researcher, each of which may give rise to potential DMCA liability: the act of circumvention; the creation of a tool used to circumvent; and the publication of the results.

With respect to the act of circumventing the access control technology (otherwise prohibited under § 1201(a)(1)), an encryption researcher should be able to circumvent the access control technology without much fear of liability if the researcher abides by the requirements spelled out in the encryption research exemption. In particular: the researcher must lawfully obtain the encrypted copy of the material he wishes to analyze; the act of circumvention must be necessary to the conduct of such research; the researcher must make a good faith attempt to obtain authorization before circumvention; and the act of circumvention must not otherwise constitute

61. Note that I focus narrowly on academic encryption researchers because much of the recent debate has focused on the impact of the DMCA on this group of researchers. This is not surprising, since nearly all sides of the debate appear to acknowledge that, whatever the impact of the DMCA might be on other encryption researchers, any impact on this core set of researchers would be very problematic—the only difference of opinion is over the scope and extent of that impact. Accordingly, I do not address the (in my view, quite legitimate) concerns that other, nonacademic encryption researchers will find it even more difficult to engage in research, except to the extent that this limitation affects academic researchers. I do not address this latter question because I eventually conclude that the DMCA in fact does affect the behavior of the core set of academic encryption researchers and that this, in itself, is extremely problematic.

copyright infringement or the violation of other applicable law.[62] In addition, the researcher should seek to satisfy the factors that a court is directed to consider in determining whether the exemption applies: the manner in which information about the research was disseminated; whether the researcher has appropriate training and experience in the field; and whether and when the researcher provided notice of the results of the research to the copyright owner.[63]

Together, these requirements raise a number of hurdles, but an academic encryption researcher should in most cases be able to overcome them. Obtaining a lawful copy will rarely be a problem for copies that are widely available to consumers.[64] A good faith attempt to obtain authorization would entail sending notice to the copyright owner, but probably not much more than that, as nothing in the statute suggests that the copyright owner must give such authorization (indeed, such a reading would be plainly inconsistent with the exemption). The provision regarding violation of other laws essentially poses no additional restriction, since a researcher violating such laws would already be separately liable.

Of these requirements, the "necessity" requirement is perhaps the most problematic. Researchers have voiced fear that they will be required to prove their actions are in fact "necessary" rather than simply "useful" or "helpful." This is a valid concern. However, in many cases researchers can meet the necessity requirement as, for example, when a researcher is testing the security of encryption as implemented on a protected copy. Almost by definition, it will be *necessary* in such a case to circumvent the protection mechanism in order to test its security. Moreover, one can reasonably expect the courts to give some deference to scientific judgments regarding what is or is not necessary in the conduct of scientific research.

The additional factors in the exemption also generally weigh in favor of academic encryption researchers. Publication of the work in an academic journal would satisfy the factor that looks to the manner of dissemination. Training in the field would be satisfied, certainly, in the case of an

62. *See* 17 U.S.C. § 1201(g)(2)(A)-(D) (2000).

63. *See id.* § 1201(g)(3)(A)-(C). I am assuming here that the researcher's activities fall within the definition of "encryption research" in accordance with § 1201(g)(1). A number of commentators have argued that the definition in the statute is too narrow. I address this issue in more detail below.

64. Note that this may arguably not be the case if a copy is obtained in violation of a shrinkwrap or other license. Moreover, this raises the broader question regarding the enforceability of shrinkwrap terms that prohibit reverse engineering or research. *See, e.g.*, Bowers v. Baystate Techs., Inc., 302 F.3d 1334, 1341 (Fed. Cir. 2002) (holding that the Copyright Act does not preempt a contractual prohibition on reverse engineering). These questions are beyond the scope of this Article.

academic encryption researcher.[65] Finally, the researcher could easily meet the third and final requirement by sending the copyright owner a copy of the research paper or otherwise notifying it of the research results. Thus, the exemption provides a fairly clear roadmap for an encryption researcher who wishes to ensure that he or she will face no liability for the act of circumvention.

Similarly, an encryption researcher should be able to create the tools necessary to engage in the act of circumvention. For example, say that a researcher, in order to crack an encrypted file, has to create a program to enable such cracking. The creation of such a program could well violate § 1201(a)(2), since it could constitute "manufactur[ing] . . . any technology . . . that . . . is primarily designed . . . for the purpose of" circumvention.[66] However, § 1201(g)(4) gives the researcher the right to "develop and deploy" circumvention technology "for the sole purpose of . . . performing the acts of good faith encryption research," thereby exempting the creation of the cracking program from liability. Moreover, the exemption permits the researcher to give the program to another person "with whom he or she is working collaboratively" for purposes of research or verification.[67]

Finally, publication of the research should be possible under the DMCA as well. The question would be whether publishing an academic paper would give rise to liability under the "tools" provision of the DMCA—i.e., would an academic paper describing weaknesses in an encryption technology constitute an "offer to the public" of "any technology . . . that . . . is primarily designed . . . for the purpose of circumventing" or "has only limited commercially significant purpose . . . other than to circumvent."[68] The argument in support of liability would be that the paper's description of the decryption technique is a "technology" and that it is either primarily designed to circumvent or has limited commercially significant use other than to circumvent.

While it is not impossible that a court would adopt such an interpretation, it is highly unlikely. First, the legislative history indicates that when

---

65. It might not be satisfied in cases where a researcher is not so clearly affiliated with an academic or other research institution. As a number of critics have pointed out, this may be quite problematic in the field of encryption research, since many discoveries are made by individuals who do not have much in the way of formal training. For present purposes, I am focusing narrowly on the question of academic encryption researchers. I will address these other concerns later in this Article.

66. § 1201(a)(2). *But see* Reese, *supra* note 40 (suggesting that the creation of a single tool might not constitute a "manufacture").

67. *Id.* § 1201(g)(4)(B).

68. *Id.* § 1201(a)(2)(A)-(B).

Congress enacted the "tools" provision, it very clearly had in mind so-called "black boxes" or other devices designed to permit consumers to engage in widespread circumvention.[69] In light of this legislative history, a court would be hard-pressed to read the provision to encompass a research paper. Second, there is a strong argument that a research paper is not "primarily designed . . . for the purpose of circumvention," even if it describes the circumvention process. Instead, the primary purpose of the paper is to advance scientific research in the field of encryption.[70] Third, such an interpretation would be in considerable tension with the terms of the encryption research exemption, which strongly suggests that the publication of research results is permissible.[71] For all of these reasons, it is highly unlikely that a court would impose liability under the DMCA for the publication of an academic paper.[72]

Further, the legislative history behind the exemption provides strong general support for exempting academic research activities and publication. It clearly evinces a concern that the DMCA should not unduly hinder encryption research, and contains many statements along these lines.[73] Any application of the DMCA to hinder legitimate research or its publication would conflict expressly with the legislative history. Thus, looking at

---

69. House Commerce Report 511, *supra* note 27, at *38 ("The Committee believes it is very important to emphasize that Section 1201(a)(2) is aimed fundamentally at outlawing so-called 'black boxes' that are expressly intended to facilitate circumvention of technological protection measures for purposes of gaining access to a work.").

70. This was the position adopted by the Department of Justice in its brief supporting dismissal of the *Felten* case:

> Plaintiffs' alleged conduct is not proscribed by the statute. [T]he DMCA prohibits trafficking in certain technologies that are primarily designed to circumvent copyright material access controls. By contrast, the Plaintiffs' alleged objective is to strengthen, not circumvent, these access controls. While Plaintiffs' computer programs have the additional capability of actually circumventing access controls, they are allegedly not designed or marketed for the purposes of actually getting access to the copyrighted material itself. They are designed and published to further scientific research into access controls. As a result, Plaintiffs' alleged conduct is not proscribed by the DMCA.

Dep't. of Justice Reply Br., Felten v. Recording Indus. Assn. (RIAA), (D.N.J. filed June 6, 2001) (No. CV-01-2669), *available at* http://www.eff.org/IP/DMCA/Felten_v_RIAA/-20011108_doj_reply_brief.html (last visited May 5, 2003) (internal citations omitted).

71. *See* § 1201(g)(3)(A) (directing courts to consider "whether the information . . . was disseminated, and if so, whether it was disseminated in a manner reasonably calculated to advance the state of knowledge or development of encryption technology").

72. The separate issue of distribution of code is dealt with below.

73. *See supra* Part II.A.

both the text and the legislative history, it is unlikely that a court would read the DMCA to cover the research activities described above.

Finally, in predicting how courts would rule on a given legal issue, one should always be aware of the factual context and, in particular, how a court would likely view the parties before it. On this score, there is every reason to expect that courts would be favorably disposed to academic encryption researchers. In particular, academic encryption researchers do not look like the "hackers" that the statute is designed to target. Although one may question the validity of this distinction as a substantive matter, it is likely that such a distinction would have an impact on a court interpreting the scope of the DMCA. Indeed, the existing DMCA litigation suggests that courts are sensitive to the identities of the alleged infringers.[74] Ultimately, the probability of a court imposing DMCA liability upon an academic encryption researcher is quite low.

Of course, a low probability of liability does not necessarily mean that copyright owners will not bring or threaten to bring claims against researchers, even if such claims are weak. As a number of DMCA critics have pointed out, eventual success in court is not required to have a devastating effect on research.[75] All that is required is the filing or even the threat of a lawsuit. As we have already seen, copyright owners have indeed made threats against academic encryption researchers.[76] Even if the substantive basis for a suit is weak, its mere filing will force a researcher to expend significant resources in response. Moreover, since no court has yet definitively interpreted the precise scope of the encryption research exemption, ambiguities in the DMCA work to the advantage of the better-funded copyright owners.

While it is true that nothing prevents copyright owners or the government from bringing weak claims, there are good reasons to believe that the

---

74. Compare, for example, the very different treatment of the "hackers" in *Universal City Studios, Inc. v. Reimerdes*, 111 F. Supp. 2d 294, 321 (S.D.N.Y. 2000), *aff'd sub nom.* Universal City Studios, Inc. v. Corley, 273 F.3d 429 (2d Cir. 2001) ("Neither of the defendants remaining in this case was or is involved in good faith encryption research . . . [a]ccordingly, defendants are not protected by section 1201(g)."), and the scientists in *Felten*. *See* Elec. Frontier Found., *Summary of Felten v. RIAA*, *at* http://www.eff.org/IP/DMCA/Felten_v_RIAA (last visited Mar. 14, 2003) ("EFF is asking the court to affirm the right of these scientists to publicly present what they have learned."). Of course, there are many other grounds for distinguishing these two cases.

75. *See, e.g.*, Wagner Comments, *supra* note 31 ("[The] threat of having to spend the time and money on a lawsuit is enough to make [encryption researchers] shy away from studying copyright protection.").

76. One example is the SDMI threat against Felten's research group. *See* Elec. Frontier Found., *Unintended Consequences*, *supra* note 51, at 2.

risks of such claims or threats are rather low. First, the risk of criminal prosecution is, in reality, quite low. Although the government initiated a criminal prosecution against Dmitri Sklyarov, the facts of that case differ from the case of an academic encryption researcher. In that case, Sklyarov worked for a for-profit company that distributed a circumvention program to consumers. For criminal liability under the DMCA to attach, the government must prove an additional element of commercial gain, which is missing in most academic encryption researcher cases. Moreover, in intellectual property cases, the United States government usually confines its criminal prosecutions to the most egregious cases of large-scale infringement, where there is clearly a profit motive. Thus, it is hard to see much realistic risk of criminal liability.

Threat of civil liability may be more of a concern, but even there, the risk of threat is reduced by a number of factors. First, the weakness of the substantive case would certainly be a factor. Second, recent cases suggest that copyright owners are sensitive to the unfavorable publicity that often follows threats to scientific research. In a number of recent cases, private parties quickly withdrew threats of DMCA suits in the wake of significant public criticism. For example, in the *Felten* litigation, public outcry over the threat of DMCA liability quickly led the RIAA to back off from its initial threat. Similarly, Hewlett-Packard recently retracted its threat of DMCA liability against a group of individuals who had discovered a security flaw in one of its products, again in response to public objections.[77] And in the Sklyarov case, although Adobe initiated the criminal investigation by complaining to the government, it quickly withdrew its support for the prosecution in response to massively unfavorable publicity.[78] Thus, the public response to weak DMCA threats directed against scientific researchers serves as an effective check against such threats.

It is true, of course, that a truly determined plaintiff could threaten or file suit in spite of a weak substantive case and bad publicity, particularly if the plaintiff feels that the stakes are high (for example, where the copyright owner already has a large installed base of copyrighted works protected by the system at issue). Thus, academic researchers are not entirely insulated from the legal risk. However, the existence of some level of risk should not completely deter future research. Many activities raise the specter of legal risks; what is important is the magnitude of the risk in comparison to the benefits. As I have argued above, although the risk is

77. *See* McCullagh, *HP Backs Down*, *supra* note 50, *at* http://news.com.com/2100-1023-947745.html.

78. The government, in the end, decided to press ahead with the case, despite Adobe's withdrawal of support.

not zero, there are good reasons based both on the law and on practical realities surrounding DMCA litigation to believe that the risk is not so severe that encryption researchers should stop conducting research altogether, particularly given the importance of such research.

The basic message here is that under the appropriate circumstances, academic encryption researchers should not be afraid to conduct and publish certain forms of research. A common and quite reasonable response to new and uncertain legislation is to hunker down and avoid exposure to any risk of legal liability, or to focus on the flaws and ambiguities in the law. Although criticism of the ambiguous and imperfect aspects of the law is important, there is also a real risk that, by focusing so much on the possibility of liability, encryption researchers will wind up censoring themselves unnecessarily. If the government and private industry groups claim that these fears are unwarranted and exaggerated,[79] then researchers should take them at their word and begin vigorously exercising their rights within the framework laid out by the DMCA. Indeed, given that academic encryption researchers are in the best position to take advantage of the exemption (and given that non-academic researchers may be less able to do so), it is particularly important that such researchers not refrain from undertaking their research.

B. The DMCA Affects the Manner in Which Research Is Conducted

I have argued above that academic encryption researchers should be able to continue to conduct and publish certain types of research without significant risk of legal liability under the DMCA. This does not mean, however, that the DMCA is therefore unobjectionable. While it permits encryption research to continue, the DMCA has a significant impact on the conditions under which such research takes place. In many ways, the debate over whether encryption researchers will be civilly or criminally liable misses the point. The answer may well be no, but the more interesting and important question is whether the DMCA affects the way in which such research is conducted and whether this more subtle effect is problematic.

---

79. *See, e.g.*, Dep't. of Justice Reply Br., *Felten* (No. CV-01-2669), *available at* http://www.eff.org/IP/DMCA/Felten_v_RIAA/20011108_doj_reply_brief.html; Recording Indus. Assn. of Am. Mem. Supp. Mot. Dismiss, *Felten* (No. CV-01-2669), *available at* http://www.eff.org/IP/DMCA/Felten_v_RIAA/20010712_riaa_mtd_memo.html); McCullagh, *Debunking DMCA Myths*, *supra* note 9, *available at* http://news.com.com/2010-12-950229.html.

As suggested above, I believe that the DMCA will have a non-trivial impact on the manner in which academic encryption research will be conducted. The impact comes from the steps that encryption researchers must take in order to avoid liability under the DMCA. The DMCA does not categorically exempt encryption research from liability. Instead, it places a number of conditions on the way such research is conducted. These conditions, while ostensibly inserted in order to sort "legitimate" from "illegitimate" encryption research, have the effect of influencing and regulating the behavior of academic encryption researchers.

First, and most critically, the DMCA will limit both the subjects of research and the universe of individuals permitted to conduct such research. As noted above, the exemption shields encryption researchers only from liability under § 1201(a) for access-control circumvention. It does not insulate researchers from liability under § 1202 for alteration of copyright management information, or under § 1201(b) for manufacturing technologies that circumvent rights-control technologies. Accordingly, researchers may well be precluded from researching such technologies. Furthermore, by privileging researchers with formal training or academic affiliations, the DMCA will prevent many existing researchers from engaging in such research.

Second, the DMCA raises a number of hurdles for a researcher to overcome before engaging in the research in the first place. One such hurdle is the need to obtain clearance for the research from the university or research organization and from legal counsel. To the extent that a researcher wishes to analyze an encrypted copyrighted work, the researcher would be well advised to obtain legal advice to ensure that the research is in compliance with the terms of the exemption. The department, university, or research organization may also have an interest in assessing its risk of liability for fostering such activities. Some university general counsel's offices may have already developed policies for DMCA cases, but most others have not. This will involve a number of additional discussions and conversations.[80]

Another initial hurdle will be to contact the copyright owner and make a good faith request for permission to engage in the act of circumvention. Failure to make such a request before engaging in the act of circumvention

80. Such discussions figured heavily in two cases I have been involved in. These discussions were particularly extensive in the *Felten* case, involving discussions with the general counsel offices of several universities, as well as private research organizations.

could, by the plain terms of the statute, make the exemption unavailable.[81] Indeed, this is another reason why clearance with counsel is important. In many cases, researchers unaware of the exemption may undertake the act of circumvention before making the request; this requirement may thus be a trap for the unwary. And although nothing in the exemption suggests that a copyright owner's authorization is necessary before proceeding, the copyright owner may seek to suppress the research or influence its content,[82] leading to additional conversations with counsel. Even if permission is eventually granted, there will be delays.

Third, the DMCA limits the universe of individuals with whom researchers can freely communicate about their research. One of the factors in the encryption research exemption focuses on the manner in which information derived from the encryption research is disseminated, i.e., whether in a manner reasonably calculated to advance the state of knowledge or in a manner that facilitates infringement. Before the DMCA, encryption researchers had few qualms discussing the results of their research, not only with academic colleagues, but also with the broader community of professional and amateur encryption researchers. As noted above, the encryption research community is characterized by much interaction between academic, professional, and "amateur" researchers. By disseminating information broadly, researchers obtain feedback and information about their research.[83] After the DMCA, however, a researcher must take care not to disclose weaknesses in encryption systems too broadly or too prematurely, since dissemination to the wrong set of individuals might constitute dissemination in a manner that facilitates infringement.[84]

Fourth, the DMCA affects the avenues through which such information is distributed. Prior to the DMCA, encryption researchers, like other computer scientists, routinely made available information about their projects on the Internet, via email, on discussion boards, or through other

---

81. *See, e.g.*, Universal City Studios, Inc. v. Reimerdes, 111 F. Supp. 2d 294, 320-21 (S.D.N.Y. 2000), *aff'd sub nom.* Universal City Studios, Inc. v. Corley, 273 F.3d 429 (2d Cir. 2001).

82. *See*, Compl. Declaratory J. and Injunctive Relief, *Felten* (No. CV-01-2669), at ¶¶ 41, 45-47 (No. CV-01-2669), *available at* http://www.eff.org/Legal/Cases/Felten_v_RIAA/20010606_eff_felten_complaint.html (technology and copyright owners asked for changes to be made in the research paper Felten's team was going to publish).

83. *See* Wagner Comment, *supra* note 31.

84. *See, e.g.*, Elec. Frontier Found., *Researcher Escapes Chilling Effect of Digital Copyright Law*, *at* http://www.eff.org/IP/DMCA/20020808_eff_bunnie_pr.html (Aug. 8, 2002) (stating that the researcher refused to respond to emails from individuals with information regarding his attempts to crack the security in the Microsoft Xbox gaming console).

more informal channels. Again, the purpose was to encourage broad dissemination of information and subject it to critique and response as part of the scientific endeavor. After the DMCA, researchers may well prefer publication in more formal channels, such as academic journals, since this type of publication would better support a finding that the information was disseminated in a manner "reasonably calculated to advance the state of knowledge."[85] Like the previous factor, the net effect here is to regulate and constrict the channels through which such information flows.

Fifth, just as the DMCA may constrict certain information flows, it forces other information flows. Prior to the DMCA, encryption researchers had no general obligation to seek permission for their research or to notify any third-parties of their results. The DMCA, however, now imposes both of these requirements, demanding that encryption researchers notify copyright holders of their intent to engage in research and requiring a good faith effort to seek authorization. In fact, this requirement is rather odd: if actual permission is required, then there is no need for an exemption. If, as is more likely, actual permission is not required, then why make the researcher ask for it?[86] The only reasonable explanation is to give the copyright owner notice of the research prior to its conduct.

In addition, the DMCA encourages disclosure of the research results to the copyright owners after the fact. In determining whether the exemption applies, a court is required to consider "whether the person provides the copyright owner of the work . . . notice of the findings and documentation of the research."[87] Thus, the DMCA encourages not only giving notice of the research results, but also handing over the details of the research. Moreover, earlier disclosure would appear to be preferable, as the DMCA expressly directs courts to look at the timing of the disclosure. Thus, there may be pressure to disclose results prior to publication, and perhaps even during the course of the research.

Sixth, and perhaps most problematically, the DMCA may have a real effect on the content of research papers. As mentioned above, it is probably a stretch to apply the "tools" provisions of the DMCA to pure research papers that do no more than simply describe weaknesses in an implemented encryption system. However, as encryption researchers have repeatedly testified before Congress, the Copyright Office, and the courts,

85. 17 U.S.C. § 1201(g)(3)(A) (2000).

86. To see the tension between this requirement and the exemption, imagine a similar requirement in the copyright fair use context. For example, a requirement that anyone intending to write a book review first make a good faith attempt to seek authorization from the author for the quotes excerpted in the book review.

87. 17 U.S.C. § 1201(g)(3)(C).

researchers routinely use code in their papers to convey ideas and illustrate techniques. Moreover, they often distribute code to others for purposes of describing their methods and seeking verification of their results.

Any such code (whether source or, more troublingly, object) would look like a "technology" as it is defined under the tools provision. The encryption research exemption only permits distribution of "tools" to collaborators, not to the wider research community.[88] Although a researcher could still argue that the research paper overall is not "primarily designed . . . for the purpose of" circumvention,[89] it is difficult to gauge how courts would treat the code. It is quite possible that a court could consider the code to be "primarily designed" for circumvention, because after all, that is its literal purpose. Accordingly, a researcher might limit the amount of code disclosed in the paper and this might affect that researcher's ability to convey ideas in the most effective and efficient manner.

Moreover, the overall structure of the encryption research exemption may have an impact on the content of research papers by involving copyright owners in the research process. The notice provisions give copyright owners an opportunity to ask for modifications of the paper in order to protect their economic interests. Indeed, in a number of cases, copyright owners have already asked for exactly these kinds of modifications.[90] A refusal to accede to "reasonable" requests for changes could be taken as a sign of lack of good faith. At the very least, this puts additional pressure on researchers to modify their papers in order to avoid trouble. The end result is that academic encryption researchers may not express themselves as freely as they would have absent the DMCA.

Thus, although academic encryption research can still occur under the DMCA, the DMCA will have a very real effect on the manner in which such research takes place. Moreover, this effect can be expected to slow the pace of discovery in this area. By limiting the subjects of research and the number of researchers, imposing additional hurdles before such research is undertaken, limiting the widespread dissemination of information, confining the avenues through which information is published, and affecting the content of published papers, the DMCA can be logically expected to raise the costs of engaging in such research. These additional barriers may be sufficiently high that some researchers may well choose to

88. *Id.* § 1201(g)(4).

89. *Id.* § 1201(a)(2)(A).

90. *See* Compl. Declaratory J. and Injunctive Relief, *Felten* (No. CV-01-2669), at ¶¶ 41, 45-47 (No. CV-01-2669), *available at* http://www.eff.org/Legal/Cases/Felten_v_RIAA/20010606_eff_felten_complaint.html.

pursue other topics, where there are no comparable hurdles.[91] Thus, even though the actual risk of liability under the DMCA may be small, the regulation of the conditions of research may nevertheless hinder encryption research.

IV. A NORMATIVE ASSESSMENT OF THE DMCA'S IMPACT

Given the DMCA's effect on the conditions under which encryption research takes place, the next question becomes: Is it worth it? The fact that the DMCA regulates encryption research does not, by itself, make such regulation problematic. It could very well be that the costs borne by encryption researchers are justified by offsetting benefits. After all, one could argue that the DMCA's requirements are reasonable regulations that balance the need for research against the harm that research could cause to the economic interests of third parties such as copyright owners.

I will argue here that, for several reasons, the burdens on encryption research described above are not justified. In advancing this argument, I focus not on a precise and detailed measuring of the costs and benefits of such regulation. Instead, I challenge the underlying idea that we should be regulating encryption research in the first place. That is, I want to expand the scope of the inquiry and ask under what circumstances we should impose burdens on scientific research in order to protect intellectual property. I suggest that the circumstances should be extremely limited—certainly far more limited than currently provided under the DMCA.

What justifies the burdens the DMCA places on academic encryption researchers? The legislative history of the DMCA suggests that one possible justification is the need to sort "legitimate" from "illegitimate" encryption research.[92] According to this justification, encryption research is extremely important and we must do everything to ensure that it can continue free and unabated. At the same time, there is a legitimate need to keep the encryption research exemption from being used as a loophole by

---

91. *See, e.g.*, Wagner Comments, *supra* note 31.

92. House Commerce Report 511, *supra* note 27, at *47. The Report states:

> The Committee recognizes that courts may be unfamiliar with encryption research and technology, and may have difficulty distinguishing between a legitimate encryption researcher and a so-called 'hacker' who seeks to cloak his activities with this defense. Section 102(g)(3) therefore contains a non-exclusive list of factors a court shall consider in determining whether a person properly qualifies for the encryption research defense.

Id. Aside from this brief mention, there are no other explanations for the specific conditions set forth in the exemption.

those who are primarily engaged not in research, but in copyright infringement. Under this view, some statutory limitations are necessary to prevent the use of the exemption as an illegitimate shield for piracy.

The problem with this justification is that the DMCA imposes far more burdens than necessary to accomplish this result. As already noted above, the DMCA does not merely sort "legitimate" from "illegitimate" research, leaving the "legitimate" research free to operate without constraint. Instead, it significantly regulates activities within the ambit of "legitimate" research. For example, the need to seek authorization from the copyright holder is hard to square with a pure "sorting" justification. Instead, it imposes an affirmative notice obligation upon researchers. The factor that encourages disclosure of research results to the copyright owner has a similar flavor. Both of these requirements do more than just help courts prevent abuse of the exemption—they regulate good faith encryption research itself.

Many other conditions in the encryption research exemption similarly have a significant impact on the activities of good faith encryption researchers. The DMCA imposes additional hurdles, which must be overcome before initiating the research. The exemption limits the scope of individuals with whom the researcher can freely communicate. It limits communication of the results of such research to certain channels and forces disclosure of information to others. Finally, it affects the content of what can be disclosed, preventing good faith researchers from communicating as freely and in as much detail as they would ordinarily like. Thus, the sorting rationale alone cannot be used to fully justify the impact the DMCA has on academic encryption research.

Given that this rationale appears insufficient, is there another way to justify the additional burdens the DMCA places on encryption research? One possibility is to argue that these burdens, whether intended or not, are justified because encryption research has the potential of harming the interests of copyright owners, and we want to permit the research but minimize the harm it causes. That is, by making available information about the weaknesses of deployed encryption systems, encryption research makes it more difficult for copyright owners to protect their works using this kind of technology. Accordingly, the DMCA effectively places a number of conditions (such as notice) on the manner in which such research takes place in order to reduce these impacts. The idea is thus not so

much to exempt good faith research entirely, but to balance the freedom to engage in such research against the interests of copyright holders.[93]

Although this justification, unlike the sorting rationale, does provide a basis for imposing additional burdens on encryption research, it is a rather radical line of reasoning. To see just how radical, consider how copyright law currently treats the question of when to impose obligations on third parties to protect intellectual property rights. This issue of third-party obligations arises in the area of new technologies and the question of when the disseminators of such technology should be contributorily or vicariously liable for infringement. The Supreme Court addressed this issue in *Sony v. Universal City Studios*,[94] in the context of the VCR. More recently, cases such as *Napster*[95] and the ongoing litigation over other peer-to-peer file sharing networks[96] as well as other digital technologies such as SonicBlue's ReplayTV[97] also grapple with this difficult issue.

The concern expressed in many of these cases is balancing the need to combat copyright infringement with the fear of burdening the development of technologies with perhaps many other, non-infringing uses. Devices such as the ones mentioned above can be used to engage in copyright infringement. At the same time, they can be used for many legitimate purposes. Imposing liability on device manufacturers may reduce copyright infringement, but at the same time impose burdens on otherwise legitimate uses of the technology and on the development of technology generally. Copyright doctrine thus attempts to carefully sort out infringing from non-infringing uses, conscious of the potential impact of imposing liability one step removed from the actual infringement. Where to draw the line is a difficult question, and much has been written on the topic.[98]

To the extent that we are concerned about the collateral impact of regulating the sale and marketing of technological devices that facilitate

---

93. Note that I am not arguing that Congress expressly thought of this justification. The legislative history actually contains very little explanation for the precise contours of the encryption research exemption. Instead, I am searching for potential justifications for these additional burdens.

94. Sony Corp. v. Universal City Studios, Inc., 464 U.S. 417 (1984).

95. A&M Records, Inc. v. Napster, Inc., 239 F.3d 1004 (9th Cir. 2001).

96. *See, e.g.*, Metro-Goldwyn-Mayer Studios, Inc. v. Grokster, Ltd., 243 F. Supp.2d 1073 (C.D. Cal. 2003).

97. *See, e.g.*, Paramount Pictures Corp. v. ReplayTV, Inc., No. CV 01-9358, 2002 WL 1301268 (C.D. Cal. Apr. 26, 2002).

98. *See, e.g.*, Stacey Dogan, *Is Napster A VCR? The Implications of Sony for Napster and Other Internet Technologies*, 52 HASTINGS L.J. 939 (2001); Richard Gilbert & Michael Katz, *When Good Value Chains Go Bad: The Economics of Indirect Liability for Copyright Infringement*, 52 HASTINGS L.J. 961 (2001).

copyright infringement, we should be even more concerned about the collateral impact of regulating encryption research. This is because, in the context of encryption research, the DMCA does not regulate merely the infringing activity, or even the technological devices that may facilitate the infringing activity. Instead, the DMCA regulates the basic scientific research that may give rise to the technological devices that can be used to facilitate infringing activity. We are thus one step even *further* removed from the difficult cases involving the regulation of technological devices, and we are *many* steps removed from the actual act of infringement. Therefore, the DMCA represents a dramatic expansion of the regulatory impact of our copyright laws.

Because we are regulating activity that is so far removed from the actual infringing activity, we need to be exceptionally careful about the unintended or collateral effects of such regulation. As copyrighted materials have become increasingly more difficult to protect, copyright owners have taken ever more drastic steps to prevent infringement. The further upstream we move from the act of infringement, however, the more likely it is that unrelated downstream activities may be unfairly affected by such regulation. This is clearly a concern in the area of basic scientific research, which occupies a privileged position precisely because its downstream effects are difficult to predict.[99] A paper studying weaknesses in an implemented encryption system may be used to create a "black-box" used to pirate copyrighted works. That same paper may, however, also spur insights in other areas of encryption research, with significant applications in completely unrelated markets and industries. The basic point is that we need to be exceptionally wary in imposing any burdens on basic scientific research because we risk affecting potentially useful unforeseen downstream activities.

To be clear, I do not argue that science is holy and untouchable, and that any regulation of scientific research is improper. The government already regulates some areas of scientific research.[100] Indeed, the government has in the past (though not without controversy) restricted the dissemination of encryption research from the U.S. to other countries, in the course of controlling the export of technologies that might affect national

99. *See, e.g.*, Steven Goldberg, *The Reluctant Embrace: Law and Science in America*, 75 GEO. L.J. 1341 (1987).

100. *See, e.g.*, Atomic Energy Act of 1954, 42 U.S.C. § 2013 (1994 & Supp. V. 1999); *Bush Praises House for Human Cloning Ban*, CNN.COM (Feb. 27, 2003), *at* http://www.cnn.com/2003/ALLPOLITICS/02/27/bush.human.cloning (discussing proposed ban on human cloning).

security.[101] Moreover, this particular type of research into implemented systems, though certainly academic, may be more intertwined with industry than other areas of pure, basic research. Thus, it would be a stretch to argue that encryption research should be categorically immune to regulation.

However, encryption research, like other basic scientific research, should only be regulated for good reason and with a properly cautious eye toward minimizing the potential collateral effects of the regulation. When the government regulates scientific research, it typically requires a significant justification, such as national security or public safety. The DMCA, by contrast, regulates research in order to protect the economic interests of third parties, namely copyright owners. Although these interests may be important, they do not rise up to the level of the other interests at stake when the government regulates scientific research. Moreover, as already detailed above, the DMCA, in pursuing this interest, does not regulate encryption research in a sufficiently careful manner.

Thus, I suggest that the government should be extremely cautious with regard to the impact of regulation on scientific research. In particular, it should be conscious of the potential downstream effects of regulation and properly sensitive to the fact that the future impact of research is difficult to predict. Accordingly, the government should carefully narrow regulation to address only the precise harm in question.[102] The baseline assumption should be that research is fully privileged. Unfortunately, in the context of the DMCA, the attitude toward encryption research has not evinced any of these careful qualities.

It is interesting to speculate about why the DMCA does not reflect this kind of careful consideration of the potential impact on scientific research. Part of the reason may simply be that Congress was not well equipped to fully appreciate the unique nature of encryption research. Encryption researchers were initially unaware of the effect that the proposed DMCA

---

101. *See, e.g.*, Junger v. Daley, 209 F.3d 481 (6th Cir. 2000); Matthew Parker Voors, *Encryption Regulation In The Wake Of September 11, 2001: Must We Protect National Security At The Expense Of The Economy?*, 55 FED. COMM. L.J. 331, 344-45 (2003); Tricia E. Black, Note, *Taking Account of the World As It Will Be: The Shifting Course of U.S. Encryption Policy*, 53 Fed. Comm. L.J. 289, 298 (2001).

102. Ideally, the regulation should also build in some flexibility to permit either courts or the Copyright Office to minimize these collateral effects as they are discovered. The DMCA does not adopt this approach, preferring instead to provide narrow, statutory exemptions. And although Congress did direct the Copyright Office to report back on the impact of the DMCA on encryption research, the timing of the report (before the effective date of the relevant DMCA provisions) suggests that Congress did not view this as a serious mechanism for generating modifications to the DMCA.

would have on their activities, and were thus late in lobbying for an exemption. Moreover, unlike other areas of scientific research, which are typically regulated by expert agencies, encryption research in the context of the DMCA did not benefit from the input of scientists within the regulatory process. Thus, despite ample testimony from encryption researchers, Congress may not have fully appreciated how the DMCA might affect such research.

Another possible explanation arises from different conceptual frameworks for information circulation. The DMCA views information as a resource to be controlled. In supporting such control, the DMCA seeks to limit circulation of information that would facilitate circumvention of technological protection measures. In this light, some limits on the circulation of scientific information might not appear to be onerous. Yet the culture of scientific research reflects a very different view of information circulation. This culture generally supports—and indeed relies upon—the free and easy circulation of information, and actively resists efforts to limit such circulation.[103] Thus, barriers on information flow that might not faze the private entities accustomed to protecting information may cause significant disruption to academic communities that rely heavily upon free circulation of information.

A simple analogy from a different context highlights the problematic impact of the DMCA on scientific research. Imagine that a company manufactures and sells bicycle locks. After years of research, the company invents a new metal alloy that is both strong and lightweight and uses this new alloy on its new locks. These locks are immensely successful. The company sells hundreds of thousands of them, and people throughout the country use them to secure bikes. A professor of materials science decides to study the properties of this new alloy, as implemented in the bike lock. She discovers that a simple combination of household chemicals, when applied to the lock, dramatically weakens it, making it easily breakable. Publication of these results would enable individuals to easily circumvent the protection offered by the locks and effectively destroy the market for these locks.[104]

---

103. *See, e.g.*, Rebecca Eisenberg, *Proprietary Rights and the Norms of Science in Biotechnology Research*, 97 YALE L.J. 177, 183-84 (1987); Harold P. Green, *The Law-Science Interface in Public Policy Decisionmaking*, 51 OHIO ST. L.J. 375 (1990). Of course, this has been changing in recent years, as the line between university and industry research has been blurring. *See, e.g.*, Eisenberg, *supra*; Arti Rai, *Regulating Scientific Research: Intellectual Property Rights and the Norms of Science*, 94 NW. U. L. REV. 77 (1999).

104. A real-life analog of this hypothetical can be found in Matt Blaze's recent discovery of weaknesses in mechanical lock systems based on a master key. *See* Matt Blaze,

What conditions should we properly place on the scientist's research and the publication of the results of the research? Would it be appropriate to impose a requirement that the scientist ask permission from the lock maker, before engaging in her research? Would it be appropriate to require disclosure of the research and results to the lock maker? To limit such research to those who have training in materials science and are affiliated with a research institution? To require that information about the weaknesses in the lock be published only in certain academic fora, but not, say, on the Internet or on an electronic bulletin board?

Many, I believe, would instinctively resist the imposition of any of these conditions upon this research. It is not difficult to see why. First, we understand the general importance of this kind of scientific investigation. Using this analogy, it is somehow easier to see that this type of research is *basic* research. It leads to the creation of important knowledge and thus should be encouraged and disseminated widely. Second, we recognize that limiting dissemination of this kind of knowledge may be harmful. Other individuals and scientists should know about the weaknesses in the alloy as soon as possible so that no one uses it for its strength without realizing this fatal defect.

Third, there is the impropriety of imposing restrictions on an unrelated third party who is pursuing knowledge. Why should we charge the researcher with the task of providing notice of her results to a private company? Why should we subject her to limits regarding to whom she can talk about her research? Fourth, and relatedly, there is a sense that the blame for the harm should rest not on the researcher, but on the company for relying upon a material that later proves to be faulty. Why should the law protect the poor technological choices by regulating the dissemination of research?

Finally, the example highlights the fact that liability for the undesirable activity should be, to the greatest extent possible, limited to the actual undesirable activity rather than to the scientific research that may enable it. It is true that publication of the research may result in some harm, as someone might use the information to break locks and steal bikes. The proper response, however, is not to regulate the creation and dissemination of the information, since this will have significant undesirable collateral effects and may ultimately result in less security. Rather, the proper response is to regulate the harm directly. Thus, it should be illegal (as it is)

Cryptology and Physical Security: Rights Amplification in Master Keyed Mechanical Locks, 1 IEEE SECURITY AND PRIVACY (forthcoming Mar./Apr. 2003), *available at* http://www.crypto.com/papers/mk.pdf (last visited May 5, 2003); *see also* John Schwartz, *Many Locks All Too Easy to Get Past*, N.Y. TIMES, Jan. 23, 2003, at C1.

to use the information to break a lock and steal a bike. Perhaps it should even be illegal to sell a "lock breaking" kit, although there might be many good reasons to provide such a kit. Certainly, however, it should not be illegal to publish basic research about weaknesses in the alloy without first jumping through many regulatory hoops. Even the placement of minimal conditions on such research seems inappropriate.

As with all analogies, there are limits, distinctions, and ways in which this analogy is not perfect. Yet I believe it captures in a concrete way what is going on in the field of encryption research under the DMCA. The DMCA regulates the conduct of basic scientific research to the benefit of private parties who *might* be adversely affected by uses of such research. The example above illustrates precisely why we should think hard before imposing even minimal burdens on basic scientific research in support of the private economic interests of unrelated third parties.

V. POTENTIAL LEGAL RESPONSES

In light of the above analysis, the DMCA should exempt, to the maximum extent possible, encryption research from liability. Instead of imposing conditions on such research, the DMCA should focus more narrowly on uses of such research that directly facilitate or encourage acts of infringement. The basic goal should be to eliminate, as much as possible, any impediments to the conduct and publication of research and focus more carefully on the precise harms at issue. In so doing, the DMCA could appropriately distinguish legitimate research from illegitimate attempts to use research as a cover for infringing activity. But the DMCA should be far more careful about doing so in a way that does not burden actual research.

There are several ways to achieve this goal. One way is through expansive judicial interpretation of the exemption, in light of the concerns expressed in this Article. For example, a liberal interpretation of the "good faith" notice requirement would reduce the burden of seeking prior authorization. In cases where the researcher, in good faith, did not know about the requirement or found the requirement too burdensome to satisfy, courts should be quick to excuse the failure and not withhold the exemption entirely. Similarly, courts should not take the failure to comply with the copyright owner's editing requests as evidence of a lack of good faith.

A court might also broadly interpret the overall good faith requirement so that it is consistent with existing encryption research practices. In determining whether research is being conducted in good faith, courts should take notice of the realities of scientific research in this field. In particular,

courts should read the "training" requirement to encompass both formal and informal types of training. Courts should also read broadly the "manner of dissemination" to acknowledge that encryption researchers often post information on websites and in other fora outside of traditional publication. This would minimize the burden on the free circulation of information within the encryption research community.

Finally, the courts should interpret the tools provisions narrowly to permit encryption researchers to exchange and publish information about their discoveries in the manner to which they have traditionally been accustomed. Thus, publication of a description should certainly be privileged. Furthermore, publication of source code, or even object code, should not violate the tools provision, insofar as the "purpose" of such publication is not to facilitate circumvention, but rather to enlarge the scope of knowledge. Such an interpretation will permit encryption researchers to communicate information about their research in the most efficient way.

If the courts were to interpret the DMCA in the fashion suggested here, the regulatory burden on encryption researchers would be greatly reduced (although not entirely eliminated).[105] Moreover, this interpretation is more in line with the stated purpose of the exemption, namely to distinguish between "legitimate" and "illegitimate" encryption research. The courts should use the standards within the research community to measure what is "legitimate" research, and once determined to be legitimate, the research should be subject to little or no regulation. Researchers should be able to disseminate information about their discoveries as broadly as possible (even if this might have the effect of harming the economic interests of intellectual property holders) without fear of liability. If the purpose of the exemption is to ensure that "good faith" encryption research can continue unfettered (rather than be regulated to protect the interests of third parties), then the suggested approach would be superior. Courts would then be truly limited to policing attempts to invoke the exemption for improper reasons.

The problem with the above approach is that it is unlikely to be implemented. For the reasons set forth in the earlier part of this Article, it is unlikely that a case involving an academic encryption researcher will be fully litigated in the above fashion. Copyright owners are reluctant to bring suit in the context of academic encryption research. Accordingly, a

105. For example, the concern about liability under § 1202 for altering copyright management information would still remain.

clarifying set of interpretations will probably not be forthcoming anytime soon.

Therefore, a better approach would be to craft a broader exemption under the DMCA for encryption research, one that gives maximum freedom to encryption researchers. A bill proposed by Senator Boucher contains such an exemption.[106] It would amend the anti-circumvention provisions of the DMCA to permit otherwise prohibited conduct when engaged "solely in furtherance of scientific research into technological protection measures."[107] As proposed, the exemption would provide a much broader exemption for scientific research, in addition to placing fewer restrictions on the conduct of research.[108] This kind of broad exemption would do a superior job of ensuring that basic scientific research is left unaffected by the DMCA.

VI. CONCLUSION

This Article has discussed a narrow—but important—issue. The world of academic encryption researchers represents a small and specific slice of the broader population affected by the DMCA. Thus, it would be tempting to dismiss concerns about laws that affect only this small slice of the population. Yet laws that raise additional barriers to scientific inquiry have the potential to affect a great many individuals who benefit from scientific discoveries. Studying the impact of the DMCA on this group of scientists illustrates how far the DMCA reaches in its attempt to protect private intellectual property rights and highlights concerns about the collateral impact of our intellectual property laws.

106. *See* Digital Media Consumers' Rights Act of 2002 (DMCRA), H.R. 5544, 107th Cong. § 5 (2002), *available at* http://www.arl.org/info/frn/copy/copytoc.html.

107. *Id.*

108. This kind of amendment has also received support from the IEEE and from Richard Clarke, the former cybersecurity "czar" for President Bush. *See IEEE-USA Position Statement: Digital Millennium Copyright Act (DMCA) Encryption Research*, *at* http://www.ieeeusa.org/forum/POSITIONS/DMCAencryption.html (June 20, 2002).

CONSUMERS AND CREATIVE DESTRUCTION: FAIR USE BEYOND MARKET FAILURE

By Raymond Shih Ray Ku[†]

ABSTRACT

For almost twenty years, the concept of market failure has defined the boundaries of fair use under copyright law. In this article Professor Ku challenges this interpretation of fair use by offering an alternative economic interpretation of the doctrine. This Article argues fair use is justified when consumer copying creatively destroys the need for copyright's exclusive rights in reproduction and distribution. This occurs when: 1) the consumer of a work makes copies of it, and 2) creation of the work does not depend upon funding derived from the sale of copies. Under these circumstances, exclusive rights in reproduction and distribution, which are conventionally justified by the need to prevent the underproduction of creative works due to free riding, are unnecessary. When both conditions are satisfied, copying does not lead to the underproduction of creative works because consumers distribute the work themselves, eliminating the need for content distributor middlemen while continuing to fund the creation of those creative works. Professor Ku argues that recognizing the process of creative destruction as fair use is not only consistent with an economic interpretation of copyright, but represents the most coherent interpretation of the consumer copying decisions handed down by the Supreme Court.

TABLE OF CONTENTS

---

† Visiting Associate Professor of Law, Cornell Law School (2002-2003); Associate Professor of Law & Director, Institute of Law, Science & Technology, Seton Hall University School of Law. I would like to thank David "Jake" Barnes and the faculties of Case Western University School of Law and Cornell Law School for their excellent comments and suggestions on earlier versions of this article. I would especially like to thank Pamela Samuelson for inviting me to participate in this symposium and the editors of the *Berkeley Technology Law Journal* for their exceptional work.

I. INTRODUCTION

Described as the most "troublesome" doctrine in copyright,[1] the doctrine of fair use is at the heart of the debate over the role digital rights management ("DRM") technologies should play in protecting creative works.[2] Some believe that DRM eliminates the need for continued recognition of the doctrine.[3] Others argue that DRM must accommodate fair use.[4] On one level, the parties to this debate disagree over the relative merits of the commons versus commodification as a means of promoting creation.[5] On another level, the debate represents a fundamental disagreement over the definition of fair use and the activities that should be considered fair. In particular, is consumer copying fair?[6] Or as Chief Justice Burger

---

1. Dellar v. Samuel Goldwyn, Inc., 104 F.2d 661, 662 (2d Cir. 1939).

2. This article does not provide a detailed discussion of DRM technologies, but instead addresses the claim that restrictions upon certain consumer uses of copyrighted works made possible by DRM are justified because those uses would otherwise infringe copyright. I leave the task of outlining the technical and ever changing world of DRM to other participants and articles in this symposium. For a non-legal, non-technical discussion of DRM, see BILL ROSENBLATT, BILL TRIPPE, & STEPHEN MOONEY, DIGITAL RIGHTS MANAGEMENT: BUSINESS AND TECHNOLOGY (M&T Books 2002).

3. *See, e.g.*, PAUL GOLDSTEIN, COPYRIGHT'S HIGHWAY: THE LAW AND LORE OF COPYRIGHT FROM GUTENBERG TO THE CELESTIAL JUKEBOX, 195-237 (Hill & Wang 1994); Tom W. Bell, *Fair Use v. Fared Use: The Impact of Automated Rights Management on Copyright's Fair Use Doctrine*, 76 N.C. L. REV. 557, 564-67 (1998); Trotter Hardy, *Property (and Copyright) in Cyberspace*, 1996 U. CHI. LEGAL. F. 217, 236, 241-42 (1996); *see also infra* Part II.B.

4. *See, e.g.*, Dan Burk & Julie Cohen, *Fair Use Infrastructure for Rights Management Systems*, 15 HARV. J. L. & TECH. 41 (2001); Pamela Samuelson, *Intellectual Property and the Digital Economy: Why the Anti-Circumvention Regulations Need to Be Revised*, 14 BERKELEY TECH. L. J. 519 (1999).

5. For extended discussions of this debate, its origins, and its implications, see GOLDSTEIN, *supra* note 3; LAWRENCE LESSIG, THE FUTURE OF IDEAS: THE FATE OF THE COMMONS IN A CONNECTED WORLD (Random House 2001); JESSICA LITMAN, DIGITAL COPYRIGHT (Prometheus Books 2001) [hereinafter LITMAN, DIGITAL COPYRIGHT]; SIVA VAIDHYANATHAN, COPYRIGHTS AND COPYWRONGS: THE RISE OF INTELLECTUAL PROPERTY AND HOW IT THREATENS CREATIVITY (NYU Press 2001).

6. Copying of this nature is often referred to as private or personal copying. *See, e.g.*, A&M Recording, Inc. v. Napster, Inc., 114 F. Supp. 2d 896, 912 (N.D. Cal. 2000) (concluding that the vast sharing of music over the Internet could not be considered pri-

once asked, is it copyright infringement when individuals make copies of copyrighted works for either their own use or to share with others?[7] How one weighs openness against commodification will substantially impact how one answers the former Chief Justice's question—perhaps the most troublesome question within this troublesome doctrine.

The casual observer might conclude that this question was answered when the United States Supreme Court held that home videotaping of copyrighted television programs was fair use,[8] or when Congress explicitly recognized the right of consumers to make home recordings of music.[9] However, more recent decisions[10] and legislation[11] cast considerable doubt on the validity of even those activities, let alone the copying and file sharing facilitated by the Internet and peer-to-peer networks.[12]

---

vate use), *aff'd*, 239 F.3d 1004 (9th Cir. 2001); GOLDSTEIN, *supra* note 3, at 129-164 (discussing private copying under copyright). Throughout this article, I use the term "consumer copying" rather than private or personal copying because it better captures the range of activities that have been considered fair in the past. Moreover, fair use does not distinguish between private or personal copying and public copying, but rather distinguishes between consumer copying and copying for financial gain. Describing this copying as private or personal erroneously suggests that fair use is based upon a right to privacy. *See infra* Part II.B.

7. *See* GOLDSTEIN, *supra* note 3, at 117-119 (describing the exchange between Chief Justice Burger and counsel during the oral arguments for Williams & Wilkins Co. v. United States, 420 U.S. 376 (1975)).

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

9. *See* Audio Home Recording Act, 17 U.S.C. § 1008 (2000) (forbidding certain infringement actions based upon the noncommercial copying of digital or analog musical recordings by consumers).

10. *See* Princeton Univ. Press v. Mich. Document Serv., 99 F.3d 1381 (6th Cir. 1996) (concluding that the creation of photocopy course packs was not fair use); Am. Geophysical Union v. Texaco Inc., 60 F.3d 913 (2d Cir. 1994) (holding that a corporation's photocopying of copyrighted articles for its researchers was not fair use); Basic Books, Inc. v. Kinko's Graphics Corp., 758 F. Supp. 1522, 1530-34, 1547 (S.D.N.Y. 1991) (same).

11. *See* Digital Millennium Copyright Act (DMCA), Pub. L. No. 105-304, 112 Stat. 2860 (1998) (codified as amended in scattered sections of 17 U.S.C. & Supp. 1999) (prohibiting, among other things, the circumvention of technologies restricting access to copyrighted works); Universal City Studios, Inc. v. Corley, 273 F.3d 429 (2d Cir. 2001) (concluding that circumventing technological measures designed to restrict access to copyrighted works was illegal even if the circumvention was for the purposes of making fair use of the work); *see also* S. 2048, 107th Cong. (2002) (proposing to require copyright security systems for all digital media devices); H.R. 5211, 107th Cong. (2002) (proposing to immunize copyright holders from liability for "disabling, interfering with, blocking, diverting, or otherwise impairing" files sharing on peer-to-peer computer networks).

12. *See* A&M Recording, Inc. v. Napster, Inc., 239 F.3d 1004 (9th Cir. 2001) (holding that peer-to-peer sharing of copyrighted music not fair use); UMG Recordings, Inc. v.

While the forces and motivations behind the movement towards eliminating fair use are varied and complex,[13] the intellectual justification offered is quite straightforward. In one of the seminal works on fair use, Wendy Gordon argued that a market-based analysis of copyright's limits would clarify fair use given copyright's underlying economic rationale.[14] The Ninth Circuit concluded that fair use should not be recognized when owners of videotape recorders recorded copyrighted television programming because the copying merely facilitated the ordinary or intrinsic use of the work.[15] Criticizing this, Gordon argued that fair use should be understood as a doctrine justifying unauthorized copying in circumstances of market failure regardless of whether the copying is for ordinary or productive uses.[16] Under this approach, fair use is an exception to the otherwise exclusive rights of copyright justified by the presence of market barriers such as high transaction costs, externalities, non-monetizable benefits, or anti-dissemination motives.[17] Thus, consumer copying and distribution of copyrighted works, such as the photocopying of scientific journals and the videotaping of television programming, could be fair use because the transaction costs associated with negotiating permission for and enforcing copyrights against such uses outweighed the benefits derived by the user and copyright owners. Treating these uses as non-infringing, fair use prevented the underutilization of these works that would otherwise have occurred.[18]

Seizing upon Gordon's work, subsequent courts and commentators have argued that consumer copying should no longer be considered fair use.[19] A central component of the market failure approach is the premise that the potential for market cures, including copyright damage awards, should be sufficient to defeat a finding of fair use. By using technological

---

MP3.COM, Inc., 92 F. Supp. 2d 349 (S.D.N.Y. 2000) (concluding that the copying of music to allow owners of that music to enjoy the works from different locations was not fair use); *see also In re* Aimster Copyright Litigation, 2002 WL 31006142 (N.D. Ill. 2002) (holding that noncommercial sharing of music by consumers represented direct copyright infringement).

13. *See generally* LITMAN, DIGITAL COPYRIGHT, *supra* note 5 (discussing some of the forces and motivations behind efforts to expand copyright).

14. Wendy J. Gordon, *Fair Use as Market Failure: A Structural and Economic Analysis of the Betamax Case and Its Predecessors*, 82 COLUM. L. REV. 1600 (1982) [hereinafter Gordon, *Fair Use*]; *see also infra* Part III.

15. *See* Sony Corp. v. Universal City Studios, Inc, 659 F.2d 963, 971-72 (9th Cir. 1981).

16. Gordon, *Fair Use*, *supra* 14, at 1652-55.

17. *Id.* at 1627-35.

18. *Id.* at 1628-30.

19. *See infra* Part II.B.

measures to restrict access and monitor uses of copyrighted works, DRM arguably eliminates the market failure created by burdensome transaction and enforcement costs.[20] If fair use is justified by market failure, DRM eliminates the need for fair use as well. We are told that DRM not only will, but should, transform creative works into private goods distributed through a system of "fared use" in which users pay for every use and every copy of a work.[21]

Not only are the conclusions and arguments offered to restrict fair use contrary to the Supreme Court's only opinion on this issue,[22] any approach that focuses exclusively on market failure overlooks the fundamental change in the economics of creation and distribution brought about by advances in technology. Elsewhere I have argued that the economics that justified copyright in the age of the printing press no longer justify a right to prohibit the consumer copying of music in the digital age.[23] Digital technology and Internet networking have creatively destroyed[24] copyright with respect to consumer sharing of music because the denial of access to music is not necessary to prevent the inefficiencies associated with free riding on the investments and efforts of others to distribute music.[25] In the digital world, the computing public internalizes the costs of creating and distributing digital music without the need for copyright's monopoly privileges or its costs.[26] Under these circumstances, consumer copying is an example of the market overcoming the public goods problem rather than market failure.

The creative destruction of copyright is not unique to the Internet. Other technologies such as the photocopier and the VCR have also led to the creative destruction of copyright. With respect to the doctrine of fair use, this observation is critical because it suggests that the Supreme Court's decisions regarding these technologies are best understood as recognizing creative destruction as fair use rather than seeing fair use as a

---

20. *Id.*

21. *See* Bell, *supra* note 3, at 567-69, 579-83 (describing "fared use").

22. Sony Corp. v. Universal City Studios, Inc., 464 U.S. 417, 450-56; *see also infra* Part III.B.

23. Raymond Shih Ray Ku, *The Creative Destruction of Copyright: Napster and the New Economics of Digital Technology*, 69 U. CHI. L. REV. 263 (2002).

24. "Creative destruction" was a term used by Joseph Schumpeter to describe what he considered to be the most important form of competition in capitalist markets, a process that "strikes not at the margins of profits and the outputs of existing firms but at their foundations." JOSEPH A. SCHUMPETER, CAPITALISM, SOCIALISM, AND DEMOCRACY 84 (Harper Perennial 1976).

25. Ku, *supra* note 23, at 293-306; *see also infra* Part IV.

26. Ku, *supra* note 23, at 293-306.

product of market failure. Moreover, concluding that creative destruction is fair use challenges the claim that the right to control copyrighted works through DRM technologies should extend "into every corner where consumers derive value from literary and artistic works."[27] In the context of this debate, although DRM may be used to limit consumer copying, it is simply inaccurate to claim that greater restrictions upon access to works are compelled by the logic of copyright. While some copyright owners may wish to expand their monopoly privileges in much the same way that members of the consuming public may want all information to be free,[28] such an expansion is not supported by either the economic theory that justifies copyright or the doctrine of copyright itself.[29]

Part II introduces the reader to copyright and the doctrine of fair use. Part II.A outlines the basics of copyright and why the monopoly rights associated with copyright are considered necessary and beneficial. Part II.B then discusses fair use and its past application to consumer copying. Specifically, Part II.B discusses the only two Supreme Court cases involving consumer copying: *Williams & Wilkins Co. v. United States*[30] and *Sony Corp. v. Universal City Studios, Inc.*[31]

Part III.A then describes Gordon's market failure interpretation of fair use. Next, Part III.B explains how the theory that fair use is only legitimate in the face of market failure has been adopted and adapted. As this discussion illustrates, more recent decisions have distinguished the Supreme Court's consumer copying precedent and restricted fair use by relying upon the market failure approach.

Part IV sets forth what I have described as the creative destruction of copyright, and argues that the two cases in which the Supreme Court addressed consumer copying are best understood if one recognizes creative destruction as a type of fair use—not that fair use is only justified by market failure. Accordingly, consumer copying—regardless of the existence of DRM technologies—should be considered fair use when two conditions are satisfied: 1) the copy is made by the consumer of the work; and 2) the

---

27. GOLDSTEIN, *supra* note 3, at 236.

28. *Cf.* Bell, *supra* note 3, at 558-59 (arguing that the true meaning of the popular Internet slogan "information wants to be free" is "people want information for free").

29. Of course, there may be other justifications expanding the protection offered to creative works, including those based upon principles of unfair competition or the moral and natural rights of authors. A discussion of those justifications, however, is beyond the scope of this article.

30. 487 F.2d 1345 (Ct. Cl. 1973), *aff'd*, 420 U.S. 376 (1975).

31. 464 U.S. 417 (1984).

creative endeavor does not depend upon funding derived from the sale of copies.

Although the presence of market failure should still be considered in determining whether a use is fair, it should not be the exclusive justification for—or explanation of—fair use. As Terry Fisher recognized, the argument that copyright owners should be entitled to revenues generated by new markets, including those created by infringers, is quite powerful and may be rebutted "[o]nly on the basis of a conception of a 'market' more restrictive than a 'group of persons who would . . . be willing to pay to see' the work."[32] According to Fisher, Justice Stevens failed to provide such a conception in *Sony*.[33] While I do not purport to defend the adequacy of the majority opinions in either *Sony* or *Williams & Wilkins*, a coherent economic approach towards fair use based upon creative destruction does emerge from these decisions without having to abandon the decisions themselves. As developed in Part IV, recognizing creative destruction as fair use is important not only because it is more consistent with the consumer copying decisions, but also because it represents an important competing conception of the market that teaches a profoundly different lesson regarding the dividing line between fair and foul.[34]

---

32. *See* William W. Fisher III, *Reconstructing the Fair Use Doctrine*, 101 HARV. L. REV. 1661, 1670-71 (1988) (recognizing the power of the argument that copyright owners should be entitled to exploit future markets including those created by infringers).

33. *Id.* at 1670-71.

34. In this respect, I disagree with Stacey Dogan who recently argued, "*Sony* is about preventing copyright holders from interfering with consumers' ability to make non-infringing uses of technology." Stacey L. Dogan, *Is Napster a VCR? The Implications of Sony for Napster and Other Internet Technologies*, 52 HASTINGS L. J. 939, 942 (2001). While *Sony* limits the right of copyright holders to interfere with the development and adoption of new technologies, it does so by limiting the types of consumer uses of technology that can be considered infringing. Similarly, I disagree with Jane Ginsburg, who suggests that the *Sony* decision is best understood as a response to the Court's perception that the copyright holders were attempting to block rather than participate in the market made possible by the VCR. *See* Jane C. Ginsburg, *Copyright and Control over New Technologies of Dissemination*, 101 COLUM. L. REV. 1613 (2001). For a different critique of Gordon's fair use approach, see Glynn S. Lunney, Jr., *Fair Use and Market Failure:* Sony *Revisited*, 82 B.U. L. REV. 975 (2002) (arguing that unauthorized copying should be considered fair when the net benefit received by society outweighs the loss generated by the copying).

II. COPYRIGHT & THE DOCTRINE OF FAIR USE

A. Copyright Basics

The United States Constitution empowers Congress, "[t]o promote the Progress of Science and useful Arts, by securing for limited Times to Authors and Inventors the exclusive Right to their respective Writings and Discoveries."[35] With regard to music, books, and movies, Congress has chosen to promote progress through the law of copyright.[36] Copyright law grants authors certain exclusive rights in their works including, as the name describes, the right to copy.[37] As the Constitution provides, copyright does not protect a natural right of authors in their works, though it is influenced by the fact that content is produced by the author's labor.[38] In-

35. U.S. CONST. art. I, § 8, cl. 8.

36. *See* 17 U.S.C. § 102 (1996) (listing the types of works protected by copyright).

37. Section 106 of the Copyright Act provides:

> [T]he owner of copyright under this title has the exclusive rights to do and to authorize any of the following:
> to reproduce the copyrighted work in copies or phonorecords;
> to prepare derivative works based upon the copyrighted works;
> to distribute copies or phonorecords of the copyrighted work to the public by sale or other transfer of ownership, or by rental, lease, or lending;
> in the case of literary, musical, dramatic, and choreographic works, pantomimes, and motion pictures and other audiovisual works, to perform the copyrighted work publicly;
> in the case of literary, musical, dramatic, and choreographic works, pantomimes, and pictorial, graphic, or sculptural works, including the individual images of a motion picture or other audiovisual work, to display the copyrighted work publicly; and
> in the case of sound recordings, to perform the copyrighted work publicly by means of a digital audio transmission.

17 U.S.C. § 106 (1996).

38. *Sony Corp. v. Universal City Studios, Inc.* states:

> The monopoly privileges that Congress may authorize are neither unlimited nor primarily designed to provide a special private benefit. Rather the limited grant is a means by which an important public purpose may be achieved. It is intended to motivate the creative activity of authors and inventors by the provision of a special reward, and to allow the public access to the products of their genius after the limited period of exclusive control has expired.

464 U.S. 417, 429 (1984); *see also* Feist Publ'ns, Inc. v. Rural Tel. Serv. Co., 499 U.S. 340, 349 (1991) ("The primary objective of copyright is not to reward the labor of authors, but "[t]o promote the Progress of Science and useful Arts."); Mazer v. Stein, 347 U.S. 201, 219 (1954) (recognizing the "economic philosophy" behind copyright); United States v. Paramount Pictures, Inc., 334 U.S. 131, 158 (1948) ("Copyright law . . . makes reward to the owner a secondary consideration."). *But see* Wendy J. Gordon, *A Property*

stead, copyright law represents a bargain between the public and the author in which the public grants authors certain exclusive rights in exchange for access to their creations.[39] This access takes two forms: access to the work during the period of exclusive rights on terms generally dictated by the author or her assigns; and unfettered access to the work after those exclusive rights have expired.[40]

This bargain is considered necessary because works of authorship share some of the characteristics of a public good. Public goods are generally defined by two traits: they are non-rivalrous, meaning that "it is possible at no cost for additional persons to enjoy the same unit of a public good";[41] and non-exclusive, meaning it is difficult to prevent people from enjoying the good. Thomas Jefferson described the public goods nature of ideas when he wrote:

> If nature has made any one thing less susceptible than all others of exclusive property, it is the action of the thinking power called an idea . . . . [T]he moment it is divulged, it forces itself into the possession of everyone, and the receiver cannot dispossess himself of it. Its peculiar character, too, is that no one possesses the less, because every other possesses the whole of it.[42]

Jefferson considered these traits beneficial because "[h]e who receives an idea from me, receives instruction himself without lessening mine; as he who lights his taper at mine, receives light without darkening me."[43]

Right in Self-Expression: Equality and Individualism in the Natural Law of Intellectual Property, 102 YALE L.J. 1533 (1993) (arguing for a natural law justification for protecting intellectual property). *See generally* Alfred C. Yen, *Restoring the Natural Law: Copyright as Labor and Possession*, 51 OHIO ST. L. J. 517 (1990) (discussing the rejection of an absolute property right in intellectual property under Anglo-American law, and proposing an alternative interpretation of natural law).

39. *See* LITMAN, DIGITAL COPYRIGHT, *supra* note 5, at 77-86.

40. *See* Jessica Litman, *The Public Domain*, 39 EMORY L. J. 965, 967-68 (1990) (describing dimensions of the public domain); Jessica Litman, *Revising Copyright Law for the Information Age*, 75 OR. L. REV. 19, 33 (1996) ("We want members of the public to be able to learn from them: to extract facts and ideas from them, to make them their own, and to be able to build on them.").

41. *See, e.g.*, RONALD V. BETTIG, COPYRIGHTING CULTURE: THE POLITICAL ECONOMY OF INTELLECTUAL PROPERTY 79-81 (1996); LITMAN, DIGITAL COPYRIGHT, *supra* note 5, at 17; Harold Demsetz, *The Private Production of Public Goods*, 13 J. L. & ECON. 293, 295 (1970); William W. Fisher, III, *Reconstructing the Fair Use Doctrine*, 101 HARV. L. REV. 1661 (1988).

42. SAUL K. PADOVER, THE COMPLETE JEFFERSON, 1011, 1015 (Duell, Sloan & Pearce ed., 1943) (quoting letter from Thomas Jefferson to Isaac McPherson, Aug. 13, 1813).

43. *Id.*

Today, we tend to be more cautious about these traits, even skeptical, because while they facilitate the widespread dissemination of ideas, they also subject public goods to "free riding." In other words, the non-rivalrous and non-exclusive characteristics of a public good increase the likelihood that some people will enjoy the benefits of the good without internalizing the costs of its production.[44] If the funding of public goods is left to the market, free riding may lead to underproduction of the good. As Gordon notes, "[i]f the creators of intellectual productions were given no rights to control the use made of their works, they might receive few revenues and thus would lack an appropriate level of incentive to create."[45] Likewise, "[f]ewer resources would be devoted to intellectual productions than their social merit would warrant."[46] Unauthorized copying, therefore, may create disincentives for investing in and distributing creative works.

Astute readers will note that, while the preceding description of public goods may describe ideas, songs, or poetry, it does not precisely describe CDs, books, or sculptures. While ideas may be non-exclusive, I can certainly keep people from reading my book or listening to my CD. As such, the CD is a private good.[47] Nonetheless, we have traditionally protected not only the song, but the CD as well. The justifications for this protection are the obvious public benefits of embodying works of authorship in a tangible medium and the threat that copying poses to the initial distributor. While a song or story may spread by word of mouth, fixing those works in tangible form facilitates the dissemination of those works to larger portions of the public while preserving the artist's original expression. However, once copies are available, it is usually inexpensive for subsequent users to copy the work. If competition from copiers drives the price of a work down to the marginal costs of the copier, it threatens the incentives to distribute the work in the first place.[48] If distributors have no incentive to make new works available, the public's access to those works will be significantly reduced. In other words, even though a CD or book is a pri-

---

44. Gordon, *Fair Use*, *supra* note 14, at 1611.

45. *Id.* at 1610.

46. *Id.*

47. BETTIG, *supra* note 41, at 80.

48. LESSIG, *supra* note 5, at 133; William M. Landes & Richard A. Posner, *An Economic Analysis of Copyright Law*, 18 J. LEGAL STUD. 325, 326 (1989); *see also* Am. Geophysical Union v. Texaco Inc., 60 F.3d 913, 927 (2d Cir. 1994) ("Ultimately, the monopoly privileges conferred by copyright protection and the potential financial rewards there from are not directly serving to motivate authors to write individual articles; rather, they serve to motivate publishers to produce journals, which provide the conventional and often exclusive means for disseminating these individual articles.").

vate good, copying still threatens the markets for these goods because their content is so easily disseminated.

Copyright, therefore, is designed not only to protect the author, but to preserve the incentives of the distributor as well. This is accomplished by granting authors a bundle of legally enforceable rights in their works similar to property rights in tangible property. Copyright owners utilize these rights to control copying, distribution, and other uses of the protected works. For instance, the author can assign or license the right to distribute to a distributor, which serves to protect the interests of both the author and the distributor. Granting copyright holders exclusive rights promotes a private market by artificially creating scarcity and exclusivity in works that would otherwise be public goods.

B. Fair Use and Consumer Copying

Since first recognized in the United States, copyright has been limited by the doctrine of fair use.[49] Often described as an "equitable rule of reason,"[50] fair use exists in part because courts have simply refused to literally construe the exclusive rights conferred by Congress.[51] As suggested by one court, given copyright's incentive-based rationale, courts have concluded that many uses of copyrighted works do not infringe copyright "because not every use of a work undermines this underlying rationale" and because the literal application of copyright could weaken other values and stifle the very progress it is supposed to promote.[52]

How one determines whether a use is fair and therefore not infringing has bedeviled courts and commentators for hundreds of years. Consistent with the equitable nature of the doctrine, whether any particular use is considered fair or unfair is decided on a case-by-case basis. While courts may consider any number of factors, four came to dominate the inquiry and were eventually codified by Congress in 1976.[53] These factors in-

---

49. *See* Basic Books, Inc. v. Kinko's Graphics Corp., 758 F. Supp. 1522, 1529 (S.D.N.Y. 1991) ("Coined as an 'equitable rule of reason,' the fair use doctrine has existed for as long as the copyright law."); *see also* Lydia Pallas Loren, *Redefining the Market Failure Approach to Fair Use in an Era of Copyright Permissions Systems*, 5 J. INTELL. PROP. L. 1, 13-15 (1997) (outlining the historical origins of fair use beginning with the English doctrine of fair abridgement).

50. Sony Corp. v. Universal City Studios, Inc., 464 U.S. 417, 454 (1984).

51. *Id.* at 791 n.29.

52. Nat'l Rifle Ass'n v. Handgun Control Fed'n, 15 F.3d 559, 561 (6th Cir. 1994).

53. The four factors were first articulated as such by Justice Story. *See* Folsom v. Marsh, 9 F. Cas. 342, 348 (C.C.D. Mass. 1841) (No. 4,901) ("In short, we must often . . . look to the nature and objects of the selections made, the quantity and value of the mate-

clude: 1) the purpose and character of the use, including whether the use is commercial or for non-profit educational purposes; 2) the nature of the copyrighted work itself, which typically involves evaluating whether the work is factual, scientific, or artistic in nature; 3) the quantitative and qualitative amount copied; and 4) the effect of the use upon the potential market for and value of the work.[54] According to Congress, § 107 was "intended to restate the present judicial doctrine of fair use, not to change, narrow, or enlarge it in any way."[55] As such, the codification did little to clarify fair use—though it did lend congressional authority to the doctrine's legitimacy. Given the case-by-case determination of fair use and lack of guidance with respect to the interpretation, weight, and application of the non-exclusive factors,[56] fair use is unsurprisingly "troubling" and "unpredictable."[57] Nonetheless, as Lloyd Weinreb noted, even though the analysis "calls for the exercise of great judicial skill, or art," principled decision-making is possible.[58] The cases dealing with consumer copying illustrate the difficulty and disagreements that make fair use such a troubling doctrine.

1. Photocopying

The first consumer copying case to reach the Supreme Court was brought by Williams & Wilkins, a publisher of medical journals and books.[59] The publisher sued the National Institute of Health (NIH) and the National Library of Medicine (NLM) for unauthorized photocopying and distribution of articles from its journals.[60] The libraries owned and operated multiple photocopying machines and maintained a policy of photocopying articles requested by NIH personnel, library patrons, or through interlibrary loan.[61] In 1970, NIH's in-house photocopying department filled 85,744 requests from NIH personnel for photocopies of journal arti-

---

rials used, and the degree in which the use may prejudice the sale, or diminish the profits, or supersede the objects, of the original work.").

54. 17 U.S.C. § 107 (1976).

55. H.R. REP. NO. 94-1476, at 66 (1976), *reprinted at* 1976 U.S.C.C.A.N. 5659, 5680; S.REP. NO. 94-473, 62 (1975).

56. *See* Basic Books, Inc. v. Kinko's Graphics Corp., 758 F. Supp. 1522, 1530 (S.D.N.Y. 1991) (recognizing that "[c]ourts and commentators disagree on the interpretation and application of the four factors").

57. Dellar v. Samuel Goldwyn, Inc., 104 F.2d 662 (2d Cir. 1939).

58. Lloyd L. Weinreb, *Fair's Fair: A Comment on the Fair Use Doctrine*, 103 HARV. L. REV. 1137, 1161 (1990).

59. Williams & Wilkins Co. v. United States, 420 U.S. 376 (1975), *aff'g*, 487 F.2d 1345 (Ct. Cl. 1973).

60. *Williams & Wilkins*, 487 F.2d at 1346-47.

61. *Id.* at 1348-49.

cles representing approximately 930,000 pages.[62] Similarly, in 1968, NLM filled approximately 120,000 interlibrary loan requests by photocopying single articles from journals.[63] While individuals requesting copies were allowed to keep them, both libraries had policies limiting excessive copying; the only general prohibition was against the copying of entire journals.[64] The Court of Claims concluded this copying was fair use, and an equally divided Supreme Court affirmed the judgment.

Two factors stand out in the Court of Claims' decision. First, the "customary facts of copyright-life"[65] clearly influenced the majority's fair use analysis. According to the court, prior to the invention of the photocopier, scholars could freely copy articles by hand or have them typed for their "personal use and files" without infringing copyright.[66] Similarly, the majority expressed great skepticism that individuals infringe copyright when making a copy on a photocopying machine for themselves or to give to others.[67] In part, the court perceived a distinction drawn by earlier copyright statutes between copying and printing books.[68] Prior to 1909, only printing, reprinting, and publishing infringed copyrighted books, while mere copying of other works, such as photographs and drawings, infringed these copyrighted works.[69] While the 1909 Act eliminated this distinction, the court believed that "there is a solid doubt whether and how far 'copy' applies to books and journals, [which] must be taken into account in measuring the outlines of 'copying' as it involves books and articles."[70] In conducting its fair use analysis, the court considered the libraries' facilitation of the photocopying as simply a more efficient means of making copies that would have otherwise been permissible since no clear history or authority prohibited the practice.[71] Consequently, the court treated the photocopying as presumptively fair absent a showing of genuine harm to the publisher or a clearer dictate from Congress.

Second, in evaluating the publisher's allegation that NIH and NLM injured Williams & Wilkins' business, the court limited the relevant or po-

---

62. *Id.* at 1348.
63. *Id.* at 1349.
64. *Id.* at 1348-49.
65. *Id.* at 1350.
66. *Id.*
67. *See id.* at 1351-52, 1353, 1355.
68. *Id.* at 1350.
69. *Id.* at 1350-51.
70. *Id.* at 1351.
71. *Cf.* Whalen v. Roe, 429 U.S. 589, 606-07 (1977) (Brennan, J., concurring) (recognizing that a practice is "not rendered [unlawful] simply because new technology makes the State's operations more efficient").

tential market to the market for medical journals. In so doing, the court explicitly rejected the district court's and publisher's positions that the relevant market includes the market or potential market for individual medical articles.[72] Measuring market harm by lost licensing opportunities for individual articles, according to the court, assumes that the publisher of the journal has the right to license those uses in the first place; this is precisely what the fair use inquiry is supposed to determine.[73] Because the authors of the medical articles are typically not paid for their contributions, but rather assigned their copyrights in return for the opportunity to be published, the copying did not threaten their incentive to write.[74] The court instead examined whether the publisher would continue to have sufficient incentive to publish the journals in their entirety.

The court also found no evidence that the copying of individual articles discouraged the publication of the journals themselves. The court found that Williams & Wilkins' subscriptions and revenues actually grew in the relevant time period, despite the copying.[75] Moreover, the majority concluded that the publisher failed to demonstrate that the libraries or researchers would have purchased additional journal subscriptions, reprints, or back issues in lieu of copying.[76] Instead, it was quite possible that researchers "might expend extra time in note-taking or waiting their turn for the library's copies of the original issues" or simply do without the articles.[77] Contributing to the fact that journals were not substitutes for the photocopies (and vice versa) were the limited budgets of the libraries and researchers, and the fact that publishers like Williams & Wilkins maintained only a small number of back issues and typically did not provide reprints of individual articles.[78] In any event, publishers would not be demonstrably better off if copying were prohibited, and arguably the state of medical research would suffer.[79] Because the copying was not a disincen-

---

72. *Williams & Wilkins*, 487 F.2d at 1356-57.

73. *Id.* at 1357 n.19.

74. *See id.* at 1359 ("The authors, with rare exceptions, are not paid for their contributions . . . . Indeed, some of the authors of the copied articles involved in this case testified at the trial that they favored photocopying as an aid to the advancement of science and knowledge.").

75. *Id.* at 1357.

76. *Id.* at 1356-57.

77. *Id.* at 1358.

78. *Id.* at 1356-57.

79. *Id.* at 1358. The opinion states:

> In the absence of photocopying, the financial, time-wasting, and other difficulties of obtaining the material could well lead, if human experience is a guide, to a simple but drastic reduction in the use of the many articles (now sought and read) which are not absolutely crucial to the

tive to publishing medical journals, the copying was ultimately considered fair. Because an equally divided Supreme Court affirmed *Williams & Wilkins*, the fair use status of consumer copying would remain in doubt until a decade later when the Court decided *Sony*.

2. The VCR

In *Sony*, Universal City Studios and Walt Disney Productions brought a copyright action against Sony Corporation and related entities for manufacturing and distributing the Betamax videocassette recorder (VCR).[80] The plaintiff studios owned the copyrights to various broadcast television programs, and argued that Sony was guilty of contributory copyright infringement because the VCR enabled millions of consumers to copy the plaintiffs' programs without authorization.[81] According to the district court's findings of fact, the average member of the public used the VCR to playback televised programs at a time subsequent to their broadcast, a practice described as "time-shifting."[82] In a five to four decision, a majority of the Supreme Court concluded that consumer videotaping of television programming for the purposes of time-shifting was fair use. Specifically, the Court held that Sony was not a contributory infringer because unauthorized time-shifting was fair and the VCR was capable of substantial non-infringing use under the staple article of commerce doctrine.[83]

Recognizing the relationship between copyright and technological change, the majority's fair use analysis was influenced by an important interpretive principle: when advances in technology challenge the application of copyright, courts should construe the fair use doctrine in light of its basic purpose to encourage creativity as a means of promoting "broad public availability of literature, music, and the other arts."[84] In light of this

---

> individual's work but are merely stimulating or helpful. The probable effect on scientific progress goes without saying, but for this part of our discussion the significant element is that plaintiff, as publisher and copyright owner, would not be better off. Plaintiff would merely be the dog in the manger.

Id.

80. Sony Corp. v. Universal City Studios, Inc., 464 U.S. 417, 419-20 (1984).

81. *Id.* at 419-20.

82. *Id.* at 421.

83. *Sony* addresses other important issues including whether the staple article of commerce doctrine from patent law should apply to claims of contributory copyright infringement and its relationship to authorized time-shifting. *Id.* at 439-41. For the purposes of this discussion, however, this article only addresses the decision regarding unauthorized copying.

84. *Id.* at 432 (quoting Twentieth Century Music Corp. v. Aiken, 422 U.S. 151, 156 (1975)).

principle, the majority rejected the studios' and dissenters' three principal arguments against fair use.

First, the Supreme Court rejected the argument that time-shifting was commercial because consumers derived economic value from the use. The studios and dissent argued that home taping was a commercial use because even if the consumer did not sell the tape, the tape was a substitute for one that may be sold by the copyright holder.[85] For example, Laurence Tribe argued, "jewel theft is not converted into a noncommercial veniality if stolen jewels are simply worn rather than sold."[86] In rejecting Tribe's argument, the Court relied upon the distinction between tangible property and the public goods nature of creative works. Justice Stevens argued that the theft of tangible property denied the owner the right to possess the property as well as the right to sell it.[87] In contrast, given the public goods nature of creative works, time-shifting deprived the owner of neither possession nor the right to sell the program to broadcasters or, for that matter, to consumers.[88]

Because time-shifting was considered a non-commercial use, the studios bore the burden of demonstrating the existence of some meaningful likelihood of future harm to their existing or potential markets.[89] Relying upon the district court's findings of fact, the Supreme Court concluded that the studios failed to make such a demonstration. According to the district court, "[h]arm from time-shifting is speculative and, at best, minimal."[90] In fact, time-shifting could benefit the studios and their advertisers by expanding the size of the viewing audience.[91] Lastly, the evidence demonstrated that television productions were more profitable than ever before and use of the VCR would not injure the studios' existing financial picture.[92]

Additionally, the studios and the dissent argued that in addition to the traditional markets for their works such as theatrical exhibition and broadcasting, home taping harmed their ability to exploit what would be a sizable market for time-shifting.[93] According to the dissent:

---

85. *See id.* at 450 n.33.
86. *See id.*
87. *See id.*
88. *Id.*
89. *Id.* at 451.
90. *Id.* at 454.
91. *Id.*
92. *Id.*
93. *Id.* at 485-86 (Blackmun, J., dissenting).

> [T]he Studios . . . demonstrate that the advent of the VTR technology created a potential market for their copyrighted programs. That market consists of those persons who find it impossible or inconvenient to watch the programs at the time they are broadcast, and who wish to watch them at other times. These persons are willing to pay for the privilege of watching copyrighted work at their convenience, as is evidenced by the fact that they are willing to pay for VTRs and tapes; undoubtedly, most also would be willing to pay some kind of royalty to copyright holders.[94]

As in *Williams & Wilkins*, the possibility of licensing and a new market for time-shifting was irrelevant to the majority's fair use analysis. Instead of rejecting the argument as circular, Justice Stevens addressed this argument rather obliquely in his discussion of the staple article of commerce doctrine. In that discussion, Justice Stevens argued that recognition of copyright liability for harm to a market for time-shifting was the functional equivalent of suggesting that copyright gave copyright holders a monopoly over the VCR.[95] The studios' willingness to license merely represented a willingness to license this claimed monopoly interest in the VCR.[96] In other words, accepting the studios' "extraordinary" argument would be the equivalent of granting all copyright owners a patent right in any technology that may be used to reproduce their works. According to the majority, such a result would extend the studios' monopoly beyond the limits conferred by copyright.[97]

Lastly, the majority rejected the argument that ordinary uses of copyrighted works could never be considered fair use. The court of appeals concluded that "when copyrighted material is reproduced for its intrinsic use, the mass copying of the sort involved in this case precludes an application of fair use."[98] According to Justice Blackmun's dissenting opinion, the categorical denial of fair use for ordinary uses is appropriate because:

> The scholar, like the ordinary users, of course could be left to bargain with each copyright owner for permission to quote from or refer to prior works. But there is a crucial difference between the scholar and the ordinary user. When the ordinary user decides that the owner's price is too high, and forgoes use of the work, only the individual is the loser. When the scholar forgoes

94. *Id.*
95. *See generally id.* at 441.
96. *Id.* at 441 n.21.
97. *Id.*
98. Sony Corp. v. Universal City Studios, Inc., 659 F.2d 963, 972 (9th Cir. 1981).

> use of a prior work, not only does his own work suffer, but the public is deprived of his contribution of knowledge. The scholar's work, in other words, produces external benefits from which everyone profits.[99]

Ordinary uses, according to the studios and dissent, create no additional public benefits to outweigh a copyright owner's interests in compensation. In rejecting this argument, the majority reasoned that the distinction between "productive" and "unproductive" uses is helpful, but not conclusive.[100] While the scholar may have a stronger claim, this tendency does not bar the possibility that ordinary uses might also be fair.[101] According to Justice Stevens, fair use is a nuanced inquiry in which neither all copyrights nor all uses are fungible.[102] If the social value in scholarship or criticism may not be dismissed, so too the social value of personal enrichment should not be ignored.[103] As such, the Court rejected a "two-dimensional" approach that categorically excludes ordinary uses from the fair use analysis.[104] In light of the Court's conclusions that time-shifting was non-commercial and did not harm the copyright owners, time-shifting was considered fair even if non-productive.

Long before Shawn Fanning created Napster and Internet peer-to-peer networks began the viral distribution of music,[105] the Supreme Court confronted the question of whether widespread copying, facilitated by certain "new" technologies (the photocopier and the VCR) could be considered fair. In both instances, consumer copying was ultimately considered fair use. Unfortunately, aside from addressing the four statutory considerations, neither majority opinion clearly articulated why consumer copying

---

99. *Sony*, 464 U.S. at 477-78 (Blackmun, J., dissenting).

100. *Id.* at 455 n.40.

101. *Id.*

102. *Id.*

103. *Id.* The opinion states:

> A teacher who copies to prepare lecture notes is clearly productive. But so is a teacher who copies for the sake of broadening his personal understanding of his specialty. Or a legislator who copies for the sake of broadening her understanding of what her constituents are watching; or a constituent who copies a news program to help make a decision on how to vote.

Id.

104. More recently, the Court reiterated its reluctance to establish categorical rules within an otherwise equitable rule of reason by rejecting the claim that all commercial uses are presumptively unfair. *See* Campbell v. Acuff-Rose Music, Inc., 510 U.S. 569 (1994).

105. *See generally* Ku, *supra* note 23 (discussing the file sharing facilitated by Napster).

should be considered fair. In *Williams & Wilkins*, an equally divided Supreme Court let stand a divided decision from the Court of Claims, and in *Sony*, a five-Justice majority reversed the Ninth Circuit in an opinion that has been roundly criticized and that could easily be limited to its facts.[106] As discussed in Part II, any lessons that might be learned from these decisions (as unsatisfactory and cryptic as they may be) have been largely ignored.

III. SONY RECAST: THE RISE OF FAIR USE AS MARKET FAILURE

A. Fair Use as Market Failure

In one of the seminal works on fair use, Wendy Gordon argued that fair use is best understood in terms of market failure.[107] According to Gordon, courts should conclude that a defendant's use is fair when: "(1) defendant could not appropriately purchase the desired use through the market; (2) transferring control over the use to defendant would serve the public interest; and (3) the copyright owner's incentives would not be substantially impaired by allowing the user to proceed."[108] Gordon suggests that the facts of *Sony* and *Williams & Wilkins* represented instances in which there were reasons to distrust the market. I emphasize that this approach is based upon the facts of those prior decisions, because not only did Gordon's article precede the Supreme Court's decision in *Sony*, her approach is both inconsistent with and critical of the type of approach taken by the majorities in both cases.

Under Gordon's approach, the presence of market failure is a "necessary precondition for premising fair use on economics grounds."[109] According to Gordon, market failures include market barriers, externalities,

---

106. *See, e.g.*, Jay Dratler Jr., *Distilling the Witches' Brew of Fair Use in Copyright Law*, 43 U. MIAMI L. REV. 233, 260-88 (1988) (criticizing *Sony*); Fisher, *supra* note 32, at 1664-92 (same); Weinreb, *supra* note 58, at 1153-54 ("Justice Stevens' arguments in favor of fair use, purportedly applying the four statutory factors, are hopelessly inadequate.").

107. Gordon, *Fair Use*, *supra* note 14. For other interpretations of fair use, see Fisher, *supra* note 32, arguing that fair use should be used to increase efficiency in the use of scarce resources or create a more just world order, Pierre N. Leval, *Toward a Fair Use Standard*, 103 HARV. L. REV. 1105 (1990), arguing that fair use should only be recognized when it promotes the production and dissemination of new creative works, Weinreb, *supra* note 58, arguing that many of the proposals for interpreting fair use unduly restrict a doctrine appropriately focused on fairness.

108. Gordon, *Fair Use*, *supra* note 14, at 1601.

109. *Id.* at 1615.

and anti-dissemination motives.[110] More recently, Gordon has described these as "technical failures."[111] Technical market failures preventing perfect competition include "endowment effects, high transaction costs between owner and user, transaction costs that prevent a user from internalizing the social benefit she generates, indivisible products, and strategic behavior."[112] The presence of such technical failures questions the market's ability to allow socially beneficial uses to occur. As a result, a judicial finding of fair use might be appropriate.[113]

With respect to new technologies, Gordon identified high transaction costs and low profits as problems when determining whether a particular use should be considered fair or infringing.

> Consider, for example, the impact of the photocopy machine or the tape recorder. Each makes it possible for individuals to make use of copyrighted works in new and potentially valuable ways. From the point of view of the individual user, the anticipated "profit" is likely to be small, so his use will be easily discouraged by transaction costs. Also, the technology's novelty may mean that the participants have no established market channels to rely on, so that the purchase of permission is likely to be cumbersome and expensive. High transaction costs and low per-transaction profits will converge. From the point of view of the copyright owner, the costs of enforcement against a diffuse group of individuals might outweigh anticipated receipts.[114]

Under Gordon's approach, the photocopier and VCR represent examples of new technologies presenting high transaction costs and low profits. Even if the researchers in *Williams & Wilkins* and the time-shifters in *Sony* wanted to obtain permission to copy the works in question, the transaction costs to obtain that permission arguably outweigh the value of that use to the individual.[115] Correspondingly, the costs of identifying and enforcing copyright against individual copiers arguably outweigh any anticipated returns to the copyright holders.[116] In light of the transaction and policing

110. *Id.* at 1627-35.

111. Wendy J. Gordon, *Market Failure and Intellectual Property: A Response to Professor Lunney*, 82 B.U. L. REV. 1031, 1037 (2002) [hereinafter Gordon, *Market Failure*] (describing the other category of market failure as one that "addresses all the normative reasons why we might not want to rely on the market, such as dissatisfaction with the pursuit of economic value").

112. *Id.*

113. *Id.*

114. Gordon, *Fair Use*, *supra* note 14, at 1628-29.

115. *Id.* at 1648-49, 1655.

116. *Id.*

costs, Gordon argued that photocopying and time-shifting were candidates for fair use. Identifying the presence of market barriers such as burdensome transaction costs, however, is not the end of the market failure inquiry.

Under Gordon's approach, if there are reasons to distrust the market, courts should consider next whether market cures other than fair use would evolve in response to the new technology. In determining whether a copyright owner's incentives would be substantially impaired, Gordon argued that courts should consider the loss of revenues from the use in question and monetary relief as an alternative to a finding of fair use.[117] Under these circumstances, relief could be limited to damages, reasonable royalty payments, or a share of the defendant's profits.[118] Not only might damage awards themselves represent a cure for market failure, they might also create incentives for defendants and copyright owners to establish institutions and agents that might reduce future transactions costs.[119] According to Gordon, courts should consider damage awards as an alternative because a premature finding of fair use might make permanent otherwise curable market failures and insulate new and valuable uses "from the stimulus of consumer demand."[120] Underlying this approach is the premise that "fairness to the copyright owner and economic efficiency demand that the assessment of his injury include the loss of revenues he would receive in the market were his entitlement to be enforced."[121] Courts should, therefore, consider the difficult factual questions of whether market cures will evolve, whether they will be practicable, and what the judiciary's role should be in bringing about such cures.[122]

With Gordon's analysis in mind, it should be no surprise that Gordon was particularly critical of the majority in *Williams & Wilkins* for not considering whether the defendants' copying threatened the potential market for licensing individual articles.[123] Presumably, Gordon would be critical of the Supreme Court's conclusions in *Sony* as well. As the following discussion demonstrates, subsequent commentators and courts have taken to heart Gordon's approach and criticisms.

---

117. *Id.* at 1623 n.126.
118. *Id.* at 1622-23.
119. *Id.* at 1655-56.
120. *Id.* at 1620-21.
121. *Id.* at 1651.
122. *Id.* at 1656.
123. *Id.* at 1651, 1655-56.

B. The Elimination of Market Failure and Fair Use

The majorities in *Williams & Wilkins* and *Sony* did not use the fair use as market failure approach and thus implicitly or explicitly rejected it. Nonetheless Gordon's approach has come to dominate the fair use doctrine. Seizing upon the potential for the licensing of new uses and DRM technologies to cure market failure, commentators, policymakers, and courts have argued for a drastic reduction, if not the wholesale elimination, of fair use.[124]

For example, building upon Gordon's work, scholars have argued that DRM should significantly narrow the fair use doctrine because DRM will help copyright owners commodify intellectual properties, making them more like private goods, which in turn will reduce the transaction costs associated with both bargaining and copyright enforcement.[125] For example, Tom Bell and Trotter Hardy argued that the Internet, online contracts, and technological measures designed to control access to copyrighted works reduce transaction costs to the point of eliminating most instances of market failure.[126] Bell posits that, trusted systems "radically reduce[] the transaction costs of licensing access to copyrighted works," and "[i]nsofar as it responds to market failure, therefore, fair use should have a much reduced scope."[127] The reduction in transaction costs will benefit the public by increasing the value of copyrighted works, thus encouraging greater production and improving distribution.[128] Correspondingly, Hardy

---

124. For an excellent discussion on the role of bargaining institutions in facilitating the licensing of intellectual property rights, see Robert P. Merges, *Contracting Into Liability Rules: Intellectual Property Rights and Collective Rights Organizations*, 84 CAL. L. REV. 1293 (1996).

125. *See, e.g.*, GOLDSTEIN, *supra* note 3, at 224 ("The capacity of the celestial jukebox to post a charge for access, and to shut off service if a subscriber does not pay his bills, should substantially reduce the specter of transaction costs. As these costs dissolve, so, too, should the perceived need for safety valves such as fair use."); Bell, *supra* note 3, at 579-80 (arguing that "automated rights management will sharply lower transaction costs for regulating the use of copyrighted materials"); Hardy, *supra* note 3, at 236 (arguing that a principal characteristic of property rules—that we rely on them in situations of low transactions costs—applies to cyberspace, because cyberspace lowers the costs of communicating); *see also* Robert P. Merges, *The End of Friction? Property Rights and Contract in the "Newtonian World of On-line Commerce"*, 12 BERKELEY TECH. L.J. 115, 130 (1997) (recognizing that "because the contemporary fair use doctrine is predicated on a market failure rationale, and because an electronic exchange potentially eliminates this market failure for digital content, fair use law will significantly shrink, or an alternative basis for fair use will be rediscovered").

126. Bell, *supra* note 3, at 581-84; Hardy, *supra* note 3, at 236-42.

127. Bell, *supra* note 3, at 583-84.

128. *Id.* at 589.

argues that because transaction costs in cyberspace "appear to be falling quite rapidly," a private property regime for intellectual works in cyberspace would best promote the development and usefulness of cyberspace by minimizing the inefficiencies of liability rules and group bargaining costs.[129]

In addition to influencing the academic discourse, the idea that fair use is justified only in response to market failure has had a profound impact on copyright policy. Most notably, through its "White Paper," the Clinton administration championed (and Congress passed) the Digital Millennium Copyright Act,[130] which, among other things, made it illegal to circumvent DRM technologies even to make fair use of copyrighted works.[131] The White Paper justified these restrictions based on the assumption that "technological means of tracking transactions and licensing will lead to reduced application and scope of the fair use doctrine."[132] In support of this position, the White Paper erroneously characterized the Supreme Court's decision in *Sony* as predicated upon market failure.[133]

Fair use as market failure has also had a dramatic impact on judicial determinations of fair use. Beginning with *Basic Books, Inc. v. Kinko's Graphics Corp.*,[134] courts began to distinguish *Williams & Wilkins* in the context of academic photocopying. These courts rejected claims of fair use by pointing to the existence of "market cures," including document delivery services that paid royalties to publishers, the emergence of licensing institutions such as the Copyright Clearance Center, and the ability to negotiate licenses directly with individual publishers.[135] According to one decision from the Second Circuit, the presence of licensing mechanisms and institutions demonstrated the existence of a market for licensing individual academic articles, and "since there currently exists a viable market for licensing these rights for individual articles, it is appropriate that po-

---

129. Hardy, *supra* note 3, at 259-60.

130. Pub. L. No. 105-304, 112 Stat. 2860 (1998) (codified as amended in scattered sections of 17 U.S.C.).

131. 17 U.S.C. §§ 1201-1205 (2000).

132. Information Infrastructure Task Force, *Intellectual Property and the National Information Infrastructure: The Report of the Working Group on Intellectual Property Rights*, 82 (Sept. 1995) [hereinafter WHITE PAPER].

133. *Id.* at 79 ("In *Sony*, the absence of any market for home taping licenses . . . led the Court to conclude that there was no cognizable harm.").

134. 758 F. Supp. 1522 (1991) (holding that a copy services production of photocopied course packets at the request of professors for use by students was not fair use).

135. *See* Princeton Univ. Press v. Michigan Document Servs., Inc., 99 F.3d 1381, 1388 (6th Cir. 1996); Am. Geophysical Union v. Texaco Inc., 60 F.3d 913, 929 (2d Cir. 1994).

tential licensing revenues for photocopying be considered in a fair use analysis."[136] Firmly embracing fair use as market failure, the court rejected the circularity argument in *Williams & Wilkins*, arguing that "it is sensible that a particular unauthorized use should be considered 'more fair' when there is no ready market or means to pay for the use, while such an unauthorized use should be considered 'less fair' when there is a ready market or means to pay for the use."[137]

The *Sony* decision has fared no better than the *Williams & Wilkins* decision. In *A&M Records, Inc. v. Napster*[138] and *UMG Recordings, Inc. v. MP3.COM, Inc.*,[139] courts rejected fair use claims with respect to the copying and distribution of digital music.[140] Napster created a peer-to-peer network that allowed users to copy their own or other people's music through the Internet.[141] MP3.COM provided its subscribers with a service that allowed them to listen to music they owned from anywhere they had Internet access.[142] In both cases, the courts concluded that the underlying use of the copies—even for listening to music one already owned from a different location (i.e., "space-shifting")—was not fair because the digital copies were substitutes for a developing market for digital downloads.[143] In *Napster* the court concluded that "[h]aving digital downloads available for free on the Napster system necessarily harms the copyright holders' attempts to charge for the same downloads."[144] Similarly, the fact that MP3.COM's service actually led to an increase in CD sales—both consumers and the company had to purchase CDs for the service to function—was irrelevant because "[a]ny allegedly positive impact of defendant's activities on plaintiffs' prior market in no way frees defendant to usurp a further market that directly derives from reproduction of plaintiffs' copyrighted works."[145] From the perspective of these courts, the music industry's willingness to license to third parties and consumers the opportunity to make and use digital music files demonstrated that market failure

136. *Am. Geophysical Union*, 60 F.3d at 930.

137. *Id.* at 931.

138. 239 F.3d 1004 (9th Cir. 2001).

139. 92 F. Supp. 2d 349 (S.D.N.Y. 2000).

140. For a more detailed discussion of these decisions and the copying facilitated by digital technologies including MP3s, see generally Ku, *supra* note 23.

141. *See Napster*, 239 F.3d at 1011-13.

142. *See MP3.COM*, 92 F. Supp. at 350.

143. *Napster*, 239 F.3d at 1017 (holding that the record supports the district court's finding that the copyright holders had expended considerable funds and effort to commence Internet sales and the licensing of digital downloads).

144. *Id.*

145. *MP3.COM*, 92 F. Supp. 2d at 352.

was not present, and the absence of market failure weighed heavily against fair use.[146]

These cases illustrate that Gordon's market failure approach has become the dominant approach for analyzing the fair use doctrine. However, as should be apparent from the discussion of *Williams & Wilkins* and *Sony* in Part II, while Gordon's approach represents her interpretation of the facts of those decisions, fair use as market failure is clearly at odds with the prevailing reasoning of those decisions. In both cases, the use of copyrighted works was considered fair despite the availability of market cures including licensing and the potential for the development of a market for individual medical articles or time-shifting. It is not surprising that in *Sony* the dissent—not the majority—embraced Gordon's work.[147] The extent of the courts' subsequent adoption of Gordon's analysis despite its inconsistency with *Sony* and *Williams & Wilkins* may be because it provides a coherent underlying rationale for these highly fact-specific decisions. It would appear that Justice Stevens failed to provide a sufficiently coherent competing rationale in *Sony*. While I do not purport to defend the adequacy of the majority opinions in either *Sony* or *Williams & Wilkins*, a coherent economic approach towards fair use based upon creative destruction does emerge from these decisions without having to abandon the decisions themselves. As developed in Part IV, recognizing creative destruction as fair use is important because it is more consistent with the Supreme Court's consumer copying decisions and it represents an important competing conception of the market.

---

146. Critics of the market failure approach, especially as the courts have applied it, criticize the tendency to focus almost exclusively on transaction costs. *See* Loren, *supra* note 49, *passim*. For example, Loren argues that this view ignores market failure attributed to the presence of external social benefits. *Id.* at 48; *see also* Ben Depoorter & Francesco Parisi, *Fair Use and Copyright Protection: A Price Theory Explanation*, 21 INT'L REV. L. & ECON. 453 (2002) (arguing the strategic behavior of the copyright holders might still create deadweight loss in a world with no transaction costs). Gordon herself is critical of this approach. *See* Gordon, *Market Failure*, *supra* note 111, at 1034 ("Transaction cost barriers are neither the only kind of economic problem to which fair use responds nor the only kind of problem to which fair use should respond."). Her original work on this issue took care to note the possibility of other market barriers including the presence of externalities or nonmonetizable interests such as contributions to "public knowledge, political debate, or human health." Gordon, *Fair Use*, *supra* note 14, at 1631-32.

147. Sony Corp. v. Universal City Studios, Inc., 464 U.S. 417, 478 (1984) (Blackmun, J., dissenting) (citing Gordon, *Fair Use*, *supra* note 14, at 1630).

IV. CREATIVE DESTRUCTION & FAIR USE

While Gordon is clearly correct when she suggests *Williams & Wilkins* and *Sony* turned upon an economic analysis of fair use, the approach was actually one of creative destruction rather than one of market failure. The following explains what I mean by the creative destruction of copyright, and its relation to what I have described elsewhere as the new economics of digital technology. The remainder of this paper argues that the process of creative destruction is not limited to digital technology and peer-to-peer networking. The photocopier and VCR worked to creatively destroy copyright as well. While neither *Williams & Wilkins* nor *Sony* expressly recognized this interpretation, creative destruction as fair use is not only consistent with the facts of both decisions, it is implicit in the decisions themselves.

A. The Creative Destruction of Copyright

Elsewhere I have argued that the copying and distribution of music facilitated by peer-to-peer networks (beginning with Napster) is not theft as the recording industry would like us to believe.[148] Instead, it is an example of a revolutionary process that should be embraced—the process of creative destruction.[149] According to Joseph Schumpeter, the most important form of competition preventing capitalist markets from becoming monopolistic is not competition regarding price, quality, and effort.[150] Rather, the "fundamental impulse that sets and keeps the capitalist engine in motion" is the process of "creative destruction,"[151] a process "that incessantly revolutionizes the economic structure [by] incessantly destroying the old one, incessantly creating a new one."[152] This form of competition "strikes not at the margins of the profits and the outputs of the existing firms but at their foundations and their very lives."[153] Under certain circumstances, new technologies that facilitate copying and distribution of creative works strike at the foundations of copyright and the industries built upon the economics of the printing press.

As discussed in Part II, copyright's *raison d'etre* is to combat free riding and the potential for the underproduction of creative works it creates. By recognizing an exclusive right to copy and distribute creative works,

148. *See generally* Ku, *supra* note 23.

149. *See* SCHUMPETER, *supra* note 24, at 81-86 (describing creative destruction); *see also* Ku, *supra* note 23, at 293-322.

150. SCHUMPETER, *supra* note 24, at 84.

151. *Id.* at 83.

152. *Id.*

153. *Id.* at 84.

copyright is a legal mechanism for ensuring that consumers of those works internalize the costs of their creation and distribution. When creative works are distributed as physical goods (e.g., CDs, books, and videotapes) copyright arguably does what it is supposed to do. The musician must have the incentive to create music, and the recording company must have the incentive to distribute that music in the form of physical goods. When tangible goods are the means of distribution, copyright encourages the substantial investment necessary to distribute music to the public by forcing consumers to internalize those costs.[154] If a competitor could free ride by selling copies of the same work without incurring the same expenses as the first distributor, competition would force prices down to the copier's costs, and the initial distributor would not be adequately compensated. Copyright discourages the subsequent copying that may threaten the initial distributor's investment.

In contrast, digital distribution challenges whether copyright is necessary when creative works are distributed as bits and bytes through the Internet and peer-to-peer networks. At first blush, the massive copying facilitated by the rapidly diminishing costs of duplicating and distributing digital works via the Internet would seem to demand increased copyright protection.[155] After all, the traditional economic analysis of copyright suggests that as the costs of copying decrease, copyright protection must increase.[156] A funny thing happens, however, as the costs of copying approach zero. Consumers begin to invest in distribution directly. In the case

---

154. *See* Ku, *supra* note 23, at 295-96. Ku states:

> In 1984, estimates suggested that it cost $125 million just to maintain a national record distribution operation. In part, this is due to the fact that unlike the author's costs of creation, which are fixed, distribution costs include not only fixed costs but also costs that increase with the number of copies produced. Each CD must be manufactured, printed, packaged, and distributed. This requires an investment in material, equipment, personnel, and facilities. Moreover, greater demand for, or wider distribution of, a CD means higher overall costs, both for making additional copies and for expanding the distribution network.

Id.

155. *See id*. at 270-74 (describing the costs of digital Internet distribution).

156. *See id*. at 296-97. Ku states:

> As the costs of copying decrease and more individuals are able to afford the technology necessary to copy, one can assume that there will be a greater number of potential copiers. So even though the copying costs for the initial distributors will decrease as well, they will be forced to compete with a greater number of copiers and copies.

See id.; Landes & Posner, *supra* 48, at 344 (arguing that "if, over time, growth in income and technological advances enlarge the size of the market for any given work, and the cost of copying declines, copyright protection should expand").

of Napster, by purchasing computers, modems, storage media, and Internet service, the consuming public funds and creates the distribution channels for digital music.[157] Consequently, with respect to distribution, the problem of free riding is arguably absent in cyberspace.

I do not mean to suggest that consumer copying is not a threat to the recording industry or other content distributors. As a matter of common sense, one's willingness to purchase music will certainly be influenced by the opportunity to obtain that music at no extra cost. File sharing, therefore, is a serious threat, one that strikes at the very foundation of a business model based upon distributing content to the public. However, copyright does not protect against this type of threat. Copyright protects the distribution of creative works in general, not a particular industry or business model. While file sharing threatens the recording industry and other content distributors, it does so because in a digital world these middlemen are largely unnecessary. Because the consuming public makes the necessary investments to distribute digital content, the distribution of content in general is not threatened. As such, Internet distribution does not suffer from the free-rider problem that plagued older methods of distribution. Under these circumstances, prohibiting consumer reproduction and distribution of creative works under copyright is unnecessary and unwarranted.[158]

Protecting distribution, however, is only half of copyright's mission. If copying threatens creation, copyright is still needed. While the artist's incentive to create has been often overshadowed by the incentives of distributors,[159] the incentive to create must still be protected even if distributors are no longer necessary. Once unbundled from distribution, however, copyright's role in promoting creation by prohibiting consumer copying is neither clear nor absolute.[160] For example, with respect to music, unre-

---

157. *See* Ku, *supra* note 23, at 301.

158. *Id.* at 300-05. Not only is file sharing not a threat to distribution, it arguably improves the public availability of music by making music available to individuals who might otherwise been unwilling or unable to pay the copyright owner's price. Correspondingly, continued recognition of copyright's exclusive rights under these circumstances would appear to undermine copyright's purpose of making works broadly available to the public. *See id*.

159. *Id.* at 294-95.

160. Copyright's reliance upon the right to exclude to transform creative works into commodities may also be undesirable. For example, I have argued that DRM technologies may be designed to facilitate the public funding of creation through a system of levies and the monitoring of aggregate Internet downloading or use. *See id.* at 311-15. Not only could this regime provide the necessary incentives to fund creation, it would do so without denying anyone access to the work because or an inability or unwillingness to

stricted consumer copying may have a marginally negative or even a positive impact upon an artist's financial incentives to create music.[161] The disconnect between copying and creativity is due to the fact that the overwhelming majority of artists earn no royalties from the sale of music.[162] Instead, most musicians earn their livelihood from live performances and other alternative sources of revenue.[163] In other words, consumer copying does little to reduce the incentives for creation because, for the most part, the creation of music is not funded by the sale of copies of that music.

Because copyright is largely irrelevant to the creation of music and is not necessary to ensure digital distribution, I have argued that the Internet and digital technology have creatively destroyed copyright as it pertains to the protection of music.[164] In other words, in light of the new economics of digital technology, the underlying economic justifications for copyright do not support restricting the sharing of music over the Internet.[165] Through ticket sales and by purchasing the components and services that create the digital distribution channels, the consuming public funds the creation and distribution of music without the costs and harms associated with legally created monopoly privileges. As discussed below, not only is this conclusion appropriate as a matter of policy, it is consistent with the doctrine of fair use as well.

B. Creative Destruction as Fair Use

The principles of creative destruction, rather than market failure, define fair use analysis when dealing with consumer copying. In other words, consumer copying should be considered fair use when two conditions are satisfied: 1) the copy is made by the consumer of the work; and

---

pay. Likewise, it would avoid the threat to privacy entailed by tracking individual downloading and usage. *See id.*; *see also* Julie E. Cohen, *A Right to Read Anonymously: A Closer Look at "Copyright Management" in Cyberspace*, 28 CONN. L. REV. 981 (1996) (arguing that DRM threatens individual privacy).

161. *See* Ku *supra* note 23, at 306-11. There are of course many non-financial incentives for becoming an artist. Advocates for greater copyright protection, however, typically assume that financial incentives dominate. For the purposes of my analysis, it is not necessary to challenge this assumption, though as John Perry Barlow has argued, it does have the tendency to equate the greatest of human achievements with pig iron. *See also* John Perry Barlow, *The Economy of Ideas*, WIRED (Mar. 1994), *available at* http://www.wired.com/wired/archive/2.03/economy.ideas.html (last visited May 4, 2003).

162. *See* Ku, *supra* note 23, at 306-08.

163. *Id.* at 308-11.

164. *See generally id.*

165. *Id.*

2) the creative endeavor does not depend upon funding derived from the sale of copies.[166]

Consistent with the overall purpose of copyright, the first condition recognizes fair use under circumstances where the consuming public is not free riding on distribution because the consumer of the work purchases the components and services that create and distribute the copies. The second condition limits findings of fair use to circumstances in which the consuming public has internalized the costs of creation in other markets. When both criteria are satisfied, copying is not evidence of market failure. Instead, it is a functioning market for creative works in which innovation rather than law addresses the underproduction problem brought about by the public goods nature of creative works. Moreover, the concept of creative destruction explains what might otherwise be considered rather cryptic or unsatisfying opinions by providing a conception of the market to compete with the one offered by the market failure approach.[167]

Both conditions are satisfied in the *Sony* and *Williams & Wilkins* decisions. The facts of *Sony* and *Williams & Wilkins* clearly satisfy the first condition for creative destruction as fair use. In each case, consumers were not free riding with respect to distribution. Instead, they made the necessary investments for distributing copyrighted works themselves. In *Sony*, having purchased televisions, VCRs, tapes, and subscribed to cable or satellite programming, consumers invested in the equipment and materials necessary to receive and record television programming. Similarly, in *Williams & Wilkins*, by purchasing photocopiers, supplies, subscriptions to the medical journals, and by paying employees to make the requested copies, NIH invested the resources needed to enable it to distribute individual medical articles. In both cases the consumers bore the marginal costs of copying and invested in the fixed costs necessary to engage in copying, explaining why the respective courts considered the copying as potentially beyond the reach of copyright.

---

166. These two conditions are by no means the exclusive or necessarily the best articulation of when the creative destruction of copyright has occurred. They represent, however, what I believe to be the clearest case for treating creative destruction as fair use. Of course, it is also accurate to suggest that when a competitor makes copies available, the public also bears the cost of distribution, albeit indirectly. However, even if the copying does not threaten future incentives to create, one might question whether for-profit distribution in competition with the creator of a work is a matter of equity rather than economics. *Cf.* Int'l News Serv. v. Associated Press, 248 U.S. 215 (1918) (recognizing a claim for unfair competition in hot news).

167. *Cf.* Fisher, *supra* note 106, at 1670-71 (criticizing the *Sony* majority for not providing a conception of the market to compete with one defined by willingness to pay).

The importance of consumers investing in the means of distribution is also consistent with the opinions themselves. In *Williams & Wilkins* the weight of this condition can be seen in the court's skepticism that Congress ever intended copyright to apply to individual copying.[168] According to the court, copyright law recognizes a distinction between copying by individuals and printing by competitors.[169] While the latter is clearly an example of free riding, the former may not be. As such, the court considered the massive photocopying engaged in by NIH and NLM equivalent to patrons of the Library of Congress photocopying entire articles, lovers exchanging copies of poems and songs, and friends sharing newspaper items.[170] While the libraries' photocopying, like these other daily uses, were candidates for fair use, the ultimate conclusion would depend upon whether the photocopying individual articles harmed journal subscriptions.[171]

The first element of creative destruction also helps tie together the pieces of Justice Stevens' majority opinion in *Sony*. Consider once again the Supreme Court's analysis of the purpose of time-shifting. As discussed earlier, the Court was unwilling to categorically exclude non-productive copying from fair use or to consider time-shifting commercial even though consumers derived an economic benefit from copying. Taken together, these conclusions make sense in light of the Court's emphasis on the public goods nature of television programming. In rejecting the jewel thief analogy, the Court clearly recognized that the public interest in protecting private goods differs from the protection of public goods. Again, one of the concerns with public goods is that free riding will discourage investment in the distribution of creative works. Having rejected the studios' limitations on the types of copying that could be considered fair, the Court could then consider the impact of time-shifting upon distribution. Moreover, because the VCR actually increased distribution by expanding access to television programming, Justice Stevens recognized that its use was actually consistent with the public interest.[172] While this public interest was "not unlimited," it supported a finding of fair use in the absence of any harm to the creation of television programming.[173]

---

168. Williams & Wilkins Co. v. United States, 487 F.2d 1345, 1350-52 (Ct. Cl. 1973).

169. *Id.* at 1351-52, 1353, 1355.

170. *Id.*

171. *Id.* at 1353.

172. Sony Corp. v. Universal City Studios, Inc., 464 U.S. 417, 454 (1984).

173. *Id.*

Arguably, the most important factor in the analysis of creative destruction as fair use is the second condition that the creative endeavor does not depend upon funding derived from the sale of copies. In *Sony*, this condition was satisfied because the facts showed that theater ticket sales and broadcast advertising funded the creation of television programming. Moreover, the studios admitted that the VCR did not reduce either theater attendance or the size of the television viewing audience.[174] In fact, some evidence suggested that by expanding the television viewing audience, time-shifting might increase ticket sales and advertising revenues.[175]

The copying at issue in *Williams & Wilkins* also satisfied the second condition. The publication of individual medical articles did not depend on sales of individual copies of those articles. Instead, the court found that publication was funded through subscriptions to the journals in which the articles appeared, and that copying of individual articles did not significantly alter the demand for journal subscription.[176] As another court explained:

> [I]n the unique world of academic and scientific articles, the effect on the marketability of composite work in which individual articles appear is not obviously related to the effect on the market for or value of the individual article. Since (1) articles are submitted unsolicited to journals, (2) publishers do not make any payment to authors for the right to publish their articles or to acquire their copyrights, and (3) there is no evidence in the record suggesting that publishers seek to reprint particular articles in new composite works . . . .[177]

This "unique world" is based largely on the fact that public and private libraries are the principal market for journal subscriptions, and have a particular interest in the availability of journals. Unlike the typical individual, libraries are not concerned with the availability of any particular article, but rather have an interest in providing for their patrons or employees with a comprehensive collection of materials including journals relevant to the library's mission.[178] As the majority recognized, while these libraries may purchase multiple subscriptions of certain publications, they will not and cannot "purchase extensive numbers of whole subscriptions . . . on the chance that an indeterminate number of articles in an indeterminate num-

174. *Id.*
175. *Id.* at 452-54.
176. *Williams & Wilkins*, 487 F.2d at 1357-58.
177. Am. Geophysical Union v. Texaco Inc., 60 F.3d 913, 928 (2d Cir. 1994).
178. *Williams & Wilkins*, 487 F.2d at 1347-49.

ber of issues will be requested at indeterminate times."[179] Correspondingly, individuals are typically interested in only a subset of the articles that appear in the journals, and are unlikely to subscribe to journals "which would only occasionally contain articles of interest to them."[180] So long as the NIH and other medical libraries continue to subscribe to the medical journals, individual articles will be published. Under these circumstances, a finding of fair use is appropriate because the creation of individual articles is funded through subscriptions to the journals in which they appear, and the copying of individual articles does not threaten the market for those journals. If *Williams & Wilkins* viewed fair use through the lens of market failure, the publisher's willingness to create a new market for individual articles through licensing should have defeated the claim. Because copying did not harm the existing market for the underlying work, the court refused to extend the copyright owners' monopoly to encompass a market for individual articles created by the photocopier.[181]

The reasons both courts offered for defining the relevant markets narrowly are also consistent with creative destruction as fair use. According to the majority in *Williams & Wilkins*, including the questioned use as one of "the potential markets" that might be harmed impermissibly assumed the ultimate conclusion of the fair use analysis.[182] Justice Stevens' opinion provides us with more insight as to why this assumption is impermissible. As discussed in Part II.B, *supra*, Justice Stevens rejected the idea of including the market for time-shifting in the analysis of market harm because it would be tantamount to granting copyright owners a monopoly in the VCR. Justice Stevens' initial interpretative principle reveals how he

---

179. *Id.* at 1357.

180. *Id.*

181. Copying may impact the availability of journals and the individual articles appearing therein if libraries that might otherwise subscribe to the journals replace their subscriptions with copies available through interlibrary loan. Institutional use of copies to substitute for subscriptions arguably would be fair use because this type of copying would not satisfy the second requirement for creative destruction as fair use. However, to the extent that the lending institution would not otherwise be able to afford a subscription, the copying may very well be justified under Gordon's market failure approach.

182. *Williams & Wilkins*, 487 F.2d at 1357 n.19. The opinion states:

> It is wrong to measure the detriment to plaintiff by loss of presumed royalty income—a standard which necessarily assumes that plaintiff has a right to issue licenses. That would be true, of course, only if it were first decided that the defendant's practices did not constitute 'fair use.' In determining whether the company has been sufficiently hurt to cause these practices to become 'unfair,' one cannot assume at the start the merit of the plaintiff's position . . . .

Id.

concluded that this exceeded the scope of copyright protection.[183] When technological change creates ambiguity, copyright must be construed in light of its basic purpose: "promoting broad availability of literature, music, and the other arts."[184] While securing a fair return for an author's labor is a means by which the public's interest may be achieved, "'[t]he sole interest of the United States and the primary object in conferring the monopoly . . . lie[s] in the general benefits derived by the public from the labors of authors.'"[185] When a use does not harm the existing incentives to create, prohibiting the use would be inconsistent with the basic purpose of copyright.[186] Such a prohibition "would merely inhibit access to ideas without any countervailing benefit."[187] In other words, while an unauthorized use might "harm" the studios by denying them revenues that they might otherwise collect, that harm is not the type that concerns copyright. The purpose of copyright is not to maximize the individual wealth of copyright holders, or even to maximize creativity. The purpose of copyright is to remove the obstacles to creation imposed by problems associated with public goods, and to put creation on an even playing field with other endeavors.[188] Because other markets funded the creation of television programming and medical journals, copyright was not necessary to achieve this objective in the new markets for time-shifting or individual medical articles, and could not justify granting copyright owners a legal monopoly in those markets.[189] As illustrated by *Sony* and *Williams & Wil-*

---

183. Sony Corp. v. Universal City Studios, Inc., 464 U.S. 417, 432 (1984) (quoting Twentieth Century Music Corp. v. Aikens, 422 U.S. 151, 156 (1975)).

184. *Id.* at 431-32.

185. *Id.* at 432 (quoting Fox Film Corp. v. Doyal, 286 U.S. 123, 127 (1932)).

186. *Id.* at 450-51.

187. *Id.*

188. As Glynn Lunney has argued:

> If we broaden copyright, we increase the economic return on any given authorship investment. We can thereby lure resources, in the form of labor and capital, away from other productive endeavors into the production of copyrighted works and lead the market to produce additional works. But to create these additional works, we must strip the resources from other sectors of the economy.

Glynn S. Lunney, Jr., *Reexamining Copyright's Incentive-Access Paradigm*, 49 VAND. L. REV. 483, 487-88 (1996). If there is a danger in being too quick to conclude that a use should be considered fair, there is also a danger in presumptively concluding that a use is within copyright's monopoly because the resulting legal monopoly might lead to more resources being devoted to creative endeavors than their social merit would warrant.

189. Of course, the fair use finding did not prevent the studios from competing in the market created by the VCR. Instead, it denied them a monopoly in that market, and subjected them to competition from time-shifters. Given the strength and size of the current

kins, consumer copying made possible by the process of creative destruction constitutes fair use.

I do not mean to suggest that expanding copyright to include control over consumer copying would not increase the incentives to create music or other works of authorship. As Jessica Litman notes, the answer to the question of "whether an increase in copyright protection will lead to the production of more or better works" is always yes.[190] Increased protection, however, also increases the costs and harms associated with the copyright monopoly.[191] Moreover, as Litman has argued:

> Whether to impose a complicated legal regime on individual consumer consumption of copyrighted works is a crucial question on which reasonable people might differ violently. Resolving it requires us to decide what we have a copyright law *for* . . . . This is not the sort of choice that it makes sense to resolve by pretending we settled it years ago. It is not the sort of choice that it makes sense to resolve by relying on linguistic fortuity.[192]

Instead, creative destruction as fair use recognizes that Congress, not the courts, generally decides the question of whether to expand copyright into markets created by new technologies. Regardless of how one interprets *Sony*, this lesson could not be clearer:

> The direction of Art. I is that *Congress* shall have the power to promote the progress of science and the useful arts. When, as here, the Constitution is permissive, the sign of how far Congress has chosen to go can come only from Congress."
>
> One may search the Copyright Act in vain for any sign that the elected representatives of the millions of people who watch television every day have made it unlawful to copy a program for later viewing at home, or have enacted a flat prohibition against the sale of machines that make such copying possible.
>
> It may well be that Congress will take a fresh look at this new technology, just as it so often has examined other innovations in

---

market for video rental and sales, it would appear that the creators of television programming are competing quite well.

190. Jessica Litman, *War Stories*, 20 CARDOZO ARTS & ENT. L.J. 337, 344 (2002) [hereinafter Litman, *War Stories*].

191. *See generally* Ku, *supra* note 23, at 317-321 (summarizing problems associated with expanding the scope of copyright).

192. Litman, *War Stories*, *supra* note 190, at 365 (emphasis added).

> the past. But it is not our job to apply laws that have not yet been written.[193]

While the doctrine of fair use should not be an obstacle if Congress decides to prohibit consumer copying,[194] it is also not a justification or vehicle for delegating the decision to courts.

V. CONCLUSION

Recognizing creative destruction as fair use rather than market failure as the sole justification for fair use radically alters the terms of today's copyright and DRM debate. Instead of justifying a never-ending expansion of control over creative works, fair use becomes a vital internal limitation upon copyright. As such, if the purpose of DRM is to protect copyright, allowances for fair use (including consumer copying) must be built into DRM technologies. Moreover, legal restrictions on fair use, like those found in the DMCA or pending before Congress, must be understood for what they are: the creation of new rights for copyright owners and the destruction of rights previously enjoyed by the public. If law and technology are used to enforce such restrictions, the public, judges, and policymakers should understand that those restrictions are not justified by copyright. Instead, they are alterations of the "traditional contours of copyright protection."[195] There can be no doubt that new technologies have the potential to "demolish a careful balancing of public good and private interests that has emerged from the evolution of" copyright.[196] We must recognize, however, that sometimes technology destroys this balance to promote the underlying purpose of copyright.

---

193. Sony Corp. v. Universal City Studios, Inc., 464 U.S. 417, 456 (1984) (internal citations omitted) (quoting Deepsouth Packing Co. v. Laitram Corp., 406 U.S. 518, 530 (1972)); *see also* Eldred v. Ashcroft, 123 S.Ct. 769, 781 (2003) (deferring to Congress on whether the Copyright Term Extension Act is a rational exercise of the legislative authority conferred by the Copyright Clause).

194. While fair use may not be an obstacle for Congress, other constitutional provisions and legal principles including the First Amendment and internal limits within the Copyright Clause, may prevent or circumscribe such an expansion.

195. *Eldred*, 123 S.Ct. at 790 (suggesting that constitutional scrutiny may be necessary if Congress were to alter "the traditional contours of copyright protection").

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

DRM AND PRIVACY

By Julie E. Cohen[†]

TABLE OF CONTENTS

I. INTRODUCTION

The future of privacy is increasingly linked to the future of copyright enforcement. In an effort to control the proliferation of unauthorized copies, and to maximize profit from information goods distributed over the Internet, copyright owners and their technology partners are designing digital rights management ("DRM") technologies that will allow more perfect control over access to and use of digital files. The same capabilities that enable more perfect control also implicate the privacy interests of users of information goods. Although DRM technologies vary considerably, at the most general level they represent an effort to reshape the prac-

---

† Professor of Law, Georgetown University Law Center. Internet: jec@law.georgetown.edu. I thank Susan Freiwald, Chris Hoofnagle, Neal Katyal, Mark Lemley, Helen Nissenbaum, Paul Schwartz, and Phil Weiser for their comments on an early version of this Article, and Andrew Crouse for his able research assistance.

tices and spaces of intellectual consumption. They also create the potential for vastly increased collection of information about individuals' intellectual habits and preferences. These technologies therefore affect both spatial and informational dimensions of the privacy that individuals customarily have enjoyed in their intellectual activity. Quite apart from the questions of intellectual property policy that surround DRM technologies, then, the proper balance between DRM and user privacy is an important question in its own right.

Interrogating the relationship between copyright enforcement and privacy raises deeper questions about the nature of privacy and what counts, or ought to count, as privacy invasion in the age of networked digital technologies. This Article begins, in Part II, by identifying the privacy interests that individuals enjoy in their intellectual activities and exploring the different ways in which certain implementations of DRM technologies may threaten those interests. Part III considers the appropriate scope of legal protection for privacy in the context of DRM, and argues that both the common law of privacy and an expanded conception of consumer protection law have roles to play in protecting the privacy of information users.

As Parts II and III demonstrate, consideration of how the theory and law of privacy should respond to the development and implementation of DRM technologies also raises the reverse question: How should the development and implementation of DRM technologies respond to privacy theory and law? As artifacts designed to regulate user behavior, DRM technologies already embody value choices. Might privacy itself become one of the values embodied in DRM design? Part IV argues that with some conceptual and procedural adjustments, DRM technologies and related standard-setting processes could be harnessed to preserve and protect privacy.

II. PRIVACY INTERESTS IN INTELLECTUAL CONSUMPTION

DRM technologies operate at the intersection of two complex and powerful constellations of privacy values. They target a set of behaviors, which I will label intellectual consumption, that often (though not always) take place within private spaces. These behaviors, in turn, concern an activity—intellectual exploration—that is widely regarded as quintessentially private. The nexus between intellectual exploration and private physical space is an important factor in the analysis of intellectual privacy. Properly understood, an individual's interest in intellectual privacy has

both spatial and informational aspects. At its core, this interest concerns the extent of "breathing space," both metaphorical and physical, available for intellectual activity. DRM technologies may threaten breathing space by collecting information about intellectual consumption (and therefore exploration) or by imposing direct constraints on these activities.

A. The Dimensions of Intellectual Privacy

Two distinct strands of privacy theory inform, and delineate the contours of, the individual interest in intellectual privacy. These strands converge to define a zone of privacy for intellectual activity that has physical as well as conceptual dimensions. Specifically, the individual interest in intellectual privacy extends both to information about intellectual consumption and exploration and to the physical and temporal circumstances of intellectual consumption within private spaces.

As conventionally understood, interests in intellectual privacy derive from interests in personal autonomy, and are primarily informational. Within Western societies, a central tenet of post-Enlightenment thought is the inviolability of each individual's rights over her own person. These rights include not only rights of bodily integrity and other corporeal rights, but also rights over one's own thoughts and personality.[1] Surveillance and compelled disclosure of information about intellectual consumption threaten rights of personal integrity and self-definition in subtle but powerful ways. Although a person cannot be prohibited from thinking as she chooses, persistent, fine-grained observation subtly shapes behavior, expression, and ultimately identity.[2] The inexorable pressure toward conformity generated by exposure, and by loss of control over uses of the gathered information, violates rights of self-determination by coopting them.

---

1. *See, e.g.*, GEORG W.F. HEGEL, PHILOSOPHY OF RIGHT (T.M. Knox trans., 1942) (1821); IMMANUEL KANT, THE METAPHYSICS OF MORALS (Mary Gregor ed. & trans., 1996) (1797); JOHN LOCKE, TWO TREATISES OF GOVERNMENT (Peter Laslett ed., 1988) (1690).

2. *See, e.g.*, Stanley I. Benn, *Privacy, Freedom, and Respect for Persons*, *in* PHILOSOPHICAL DIMENSIONS OF PRIVACY: AN ANTHOLOGY 223 (Ferdinand David Schoeman ed., 1984) [hereinafter PHILOSOPHICAL DIMENSIONS OF PRIVACY]; Jeffrey H. Reiman, *Privacy, Intimacy, and Personhood*, *in* PHILOSOPHICAL DIMENSIONS OF PRIVACY, *supra*, at 300; Anita L. Allen, *Coercing Privacy*, 40 WM. & MARY L. REV. 723, 754-55 (1999); Julie E. Cohen, *Examined Lives: Informational Privacy and the Subject as Object*, 52 STAN. L. REV. 1373, 1424-28 (2000) [hereinafter Cohen, *Examined Lives*]; Julie E. Cohen, *A Right to Read Anonymously: A Closer Look at "Copyright Management" in Cyberspace*, 28 CONN. L. REV. 981, 1006-14 (1996) [hereinafter Cohen, *A Right to Read Anonymously*]; Ruth Gavison, *Privacy and the Limits of Law*, 89 YALE L.J. 421 (1980); Seth F. Kreimer, *Sunlight, Secrets, and Scarlet Letters: The Tension Between Privacy and Disclosure in Constitutional Law*, 140 U. PA. L. REV. 1, 59-71 (1991).

Additionally, surveillance and exposure devalue the fundamental dignity of persons by reducing the exposed individuals to the sum of their "profiles."[3] For these reasons, in circumstances where records of intellectual consumption are routinely generated—libraries, video rental memberships, and cable subscriptions—society has adopted legal measures to protect these records against disclosure.[4] Privacy rights in information about intellectual activities and preferences preserve the privacy interest in (metaphoric) breathing space for thought, exploration, and personal growth.

The second strand of privacy theory that relates to intellectual privacy concerns privacy within physical spaces. Within Western societies, tradition and social practice reserve certain types of "private space" to the individual or the family. Chief among these is the home, which is conceived as a place of retreat from the eyes of the outside world.[5] Some privacy skeptics argue that rules about entitlements to privacy within certain spaces overlap substantially with property-based entitlements to control access to private homes or offices.[6] Yet the correspondence between ownership and spatial privacy is imperfect. Not every invasion of a residential property interest is an invasion of privacy; for example, most people do not think that a nuisance, such as excessive noise or noxious fumes, is also a privacy invasion.[7] And individuals can have privacy expectations in spaces that they do not own or rent, such as public restrooms, dressing

---

3. *See* Benn, *supra* note 2; *cf.* JEFFREY ROSEN, THE UNWANTED GAZE: THE DESTRUCTION OF PRIVACY IN AMERICA (2000) (arguing that privacy protects the individual interest in not being judged "out of context"); Radhika Rao, *A Veil of Genetic Ignorance? Protecting Privacy as a Mechanism to Ensure Equality* (2003) (unpublished manuscript, on file with the author) (arguing that privacy is grounded in equality interests).

4. *See, e.g.*, Video Privacy Protection Act of 1988, Pub. L. 100-618 (codified at 18 U.S.C. § 2710 (2000)); Cable Communications Policy Act of 1984, Pub. L. 98-549 (codified at 47 U.S.C. § 551 (2000)); Cohen, *A Right to Read Anonymously*, *supra*, note 2, at 1031 n.213 (collecting state statutes safeguarding the privacy of library patrons).

5. Commentators differ on how far back in time this tradition extends, and it is also true that wealthier individuals, families, and groups, who can more easily afford to purchase space, historically have enjoyed more of this sort of privacy. Nonetheless, commitment to (varying degrees of) spatial privacy is at least a distinguishing characteristic of modern societies.

6. *See, e.g.*, Judith Jarvis Thomson, *The Right to Privacy*, *in* PHILOSOPHICAL DIMENSIONS OF PRIVACY, *supra* note 2, at 272.

7. *Cf.* Gavison, *supra* note 2, at 436-39 ("There are no good reasons . . . to expect any similarity between intrusive smells or noises and modes of acquiring information about or access to an individual."); Ferdinand David Schoeman, *Privacy: Philosophical Dimensions of the Literature*, *in* PHILOSOPHICAL DIMENSIONS OF PRIVACY, *supra* note 2, at 1, 27-28 (demonstrating that not every privacy invasion directed at private property also invades the property interest).

rooms, and telephone booths.[8] Acknowledgment of these expectations suggests a fairly broad consensus that the interests protected by "privacy" and "property" are different. Rules and traditions about freedom within private spaces concern not only property interests, but also guarantees of literal, physical breathing space for individual behavior. Sheltered behaviors may include both those that are aberrant when measured against some dominant social norm and those that simply are not intended for general public consumption. One may, for example, walk around nude inside one's own home, even though one is not free to do so in public.

Among the behaviors shielded by spatial privacy are those relating to activities of the mind. Just as spatial privacy allows for physical nudity, so it also allows for metaphorical nudity; behind closed doors, one may shed the situational personae that one adopts with co-workers, neighbors, fellow commuters, or social acquaintances, and become at once more transparent and more complex than any of those personae allows.[9] Spatial privacy affords the freedom to explore areas of intellectual interest that one might not feel as free to explore in public. It also affords the freedom to dictate the circumstances—the when, where, how, and how often—of one's own intellectual consumption, unobserved and unobstructed by others. In many nonprivate spaces, this freedom is absent or compromised. For example, one may enter a library or a bookstore only during business hours, and copyright law restricts the ability to watch movies on the premises of video rental establishments.[10] The essence of the privacy that private space affords for intellectual consumption is the absence of such lim-

8. *See, e.g.*, Katz v. United States, 389 U.S. 347 (1967) (holding that a person has a reasonable expectation of privacy while using a public telephone booth); Doe by Doe v. B.P.S. Guard Servs., Inc., 945 F.2d 1422 (8th Cir. 1991) (holding that surreptitious videotaping of fashion models in their dressing room was an invasion of privacy); Benitez v. KFC Nat'l Mgmt. Co., 714 N.E.2d 1002 (Ill. App. Ct. 1999) (holding that female employees' allegations that employer spied on them through hole in ceiling of women's restroom stated a claim for invasion of privacy); Harkey v. Abate, 346 N.W.2d 74 (Mich. Ct. App. 1983) (holding that installation of hidden viewing device in public restroom at skating rink invaded privacy). *But see* Hougum v. Valley Mem'l Homes, 574 N.W.2d 812 (N.D. 1998) (no invasion of privacy where employee only unintentionally observed man masturbating in public restroom); Elmore v. Atl. Zayre, Inc., 341 S.E.2d 905, 907 (Ga. Ct. App. 1986) (holding that rights of privacy in store restrooms may be outweighed by store's interest in deterring crime).

9. *Cf.* ERVING GOFFMAN, THE PRESENTATION OF SELF IN EVERYDAY LIFE (1959) (exploring the different ways in which individuals present themselves in different contexts); ALAN F. WESTIN, PRIVACY AND FREEDOM 32-42 (1970) (arguing that privacy enables breathing space for emotional release, autonomous development, and self-evaluation).

10. *See* Columbia Pictures Indus., Inc. v. Aveco, Inc., 800 F.2d 59 (3d Cir. 1986); Columbia Pictures Indus., Inc. v. Redd Horne, Inc., 749 F.2d 154 (3d Cir. 1984).

its. The interest in unfettered intellectual exploration includes an interest in the unfettered ability to use and enjoy intellectual goods within those spaces.[11]

B. DRM Technologies and Intellectual Privacy

DRM technologies are poised to affect both the spatial and the informational dimensions of intellectual privacy. Both by directly constraining private behaviors related to intellectual consumption and by enabling creation of detailed and permanent records of such consumption, these technologies have the potential to change dramatically the way people experience intellectual goods. Whether they will do so in a way that undermines either set of intellectual privacy values is an important question. To answer it, we must consider each of the general functions that a DRM technology might perform.

1. Constraint

Some DRM technologies are designed to set and automatically enforce limits on user behavior. For example, a music delivery format might prevent copying, including copying for "space-shifting" purposes, or might restrict the types of devices that can be used for playback.[12] The "content scrambling system" (CSS) algorithm used on DVDs does both of these things, and also implements a "region coding" compatibility system designed to ensure that DVDs intended for use in one geographic region (e.g., North America) cannot be played on equipment sold elsewhere.[13]

Technologies that constrain user behavior narrow the zone of freedom traditionally enjoyed for activities in private spaces, and in particular for activities relating to intellectual consumption within those spaces. In so

---

11. *Cf.* Stanley v. Georgia, 394 U.S. 557, 563-65 (1969) (recognizing "the right to satisfy [one's] intellectual and emotional needs in the privacy of [one's] own home"). Out of an abundance of caution, I should note that this interest in unrestricted intellectual consumption neither presupposes nor implies a broader interest in wholly unrestricted behavior that would shield, for example, crimes against persons committed in private spaces.

12. *See* Amy Harmon, *CD-Protection Complaint Is Settled*, N.Y. TIMES, Feb. 25, 2002, at C8; P.J. Huffstutter & Jon Healey, *Suit Filed Against Record Firms*, L.A. TIMES, June 14, 2002, at C3; Brenda Sandburg, *Milberg Weiss Weighs In Over No-Copy Audio: Discs Are Misleading and Defective, Suit Says*, THE RECORDER, June 17, 2002, at 1; Joe Wilcox, *Microsoft Protecting Rights—Or Windows?*, CNET NEWS.COM (Feb. 3, 2003), *at* http://news/com.com/2100-1023-983017.html.

13. *See* Matt Lake, *How It Works: Tweaking Technology to Stay Ahead of the Film Pirates*, N.Y. TIMES, Aug. 2, 2001, at G9; Doug Mellgren, *Acquittal in DVD Decoding: Norwegian Teen Created Program So He Could View Film on Computer*, CHARLOTTE OBSERVER, Jan. 8, 2003, at 3D; John Borland, *Studios Race to Choke DVD Copying*, CNET NEWS.COM (Feb. 4, 2002), *at* http://news.com.com/2100-1023-828449.html.

doing, they decrease the level of autonomy that users enjoy with respect to the terms of use and enjoyment of intellectual goods. Does this constriction also amount to an invasion (or, more neutrally, a lessening) of privacy? That depends on how privacy and its absence are defined.

It is hard to argue that a copy-protection device "intrudes on seclusion" in the precise manner contemplated by the Prosserian tort of that name.[14] The tort theory of spatial privacy envisions "seclusion" as physical isolation from human observation. The sort of intrusion cognizable as privacy invasion generally involves direct human agency and at least the possibility of a human observer.[15] Technologies of direct constraint, in contrast, operate automatically and without recourse to an external controller. But to say that these technologies therefore cannot "intrude" begs the question whether standards devised by courts to remedy invasions of private space in the predigital age should be the touchstone for assessing diminutions of spatial privacy in the digital age. A less precedent-bound conceptualization of privacy might frame matters differently.

More abstractly, many philosophers conceive of "privacy" as a condition of inaccessibility or limited accessibility to the rest of the world.[16] Invasions of privacy involve rendering the individual more accessible to others in some way. Technologies of direct constraint do not map especially well to this theory, either. Copy-control restrictions and similar constraints do not render individuals who purchase restricted works more accessible to others in any particularized way; they simply carry out their assigned tasks. If I buy a copy-protected music CD and play it in my living room, I and my living room are no more accessible to the copyright owners of the various musical works and sound recordings than the day before I made my purchase.

Conceptualizing loss of privacy in terms of either intrusion or particularized accessibility, however, misses an important aspect of the dynamic established by DRM technologies of direct constraint. From an informa-

---

14. *See* W. PAGE KEETON ET AL., PROSSER AND KEETON ON TORTS § 117 (5th ed. 1984); William L. Prosser, *Privacy*, 48 CAL. L. REV. 383, 389 (1960) (summarizing evolution of privacy causes of action).

15. *See, e.g.*, Ass'n Servs., Inc. v. Smith, 549 S.E.2d 454, 459 (Ga. Ct. App. 2001) (holding that trespassing upon private property while conducting surveillance could constitute intrusion upon seclusion); Miller v. Brooks, 472 S.E.2d 350 (N.C. App. 1996) (holding that placing a video camera in plaintiff's bedroom and going through his mail could constitute intrusion upon seclusion); Clayton v. Richards, 47 S.W.3d 149 (Tex. App. 2001) (holding that placing a video camera in plaintiff's bedroom could constitute intrusion upon seclusion).

16. *See, e.g.*, ANITA ALLEN, UNEASY ACCESS: PRIVACY FOR WOMEN IN A FREE SOCIETY (1988); Gavison, *supra* note 2, at 423; Schoeman, *supra* note 2, at 2-4.

tion provider's perspective, there are several possible ways to respond to the problem of policing user behavior under conditions of limited accessibility. One is to develop DRM technologies that enable surveillance; those technologies are discussed below. Another—the strategy of direct constraint considered here—is to restrict the range of permitted behaviors in a way that is known *ex ante*, thereby eliminating any need for intrusive monitoring.[17] This strategy subverts the logic of privacy-as-inaccessibility. I and my living room may be no more accessible to the copyright owners of the copy-protected music CD than before I bought it, but that does not matter; the feasible uses of the CD are known, and so the question of particularized accessibility to me is moot. Yet from an information user's perspective, it is hard to see the result as non-invasive; if anything, it is more efficiently invasive than a surveillance strategy would be.

Focusing narrowly on "intrusion" or "accessibility" also ignores the complex intersectionality of the privacy concerns implicated by DRM technologies. This approach reduces even the interest in spatial privacy to a primarily informational one, and excludes consideration of the other intellectual privacy values that spatial privacy serves. In particular, as already noted, intellectual privacy resides partly in the ability to exert (a reasonable degree of) control over the physical and temporal circumstances of intellectual consumption within private spaces. This argument has points of commonality with a strand of privacy theory that emphasizes decisional autonomy as the basis for at least some privacy rights. Some philosophers argue that where certain deeply personal activities are concerned, privacy denotes not only a condition of (relative) inaccessibility, but also a zone of noninterference with individual choice.[18] The usual examples relate to rights to control one's own person (e.g., decisions about reproduction, or about intimate relationships), but one might extend the argument to encompass rights to control one's own intellectual development. My argument that intellectual privacy resides, in part, in freedom from physical or architectural constraint diverges from those arguments to

17. *Cf.* LAWRENCE LESSIG, CODE AND OTHER LAWS OF CYBERSPACE (1999) (elaborating the ways in which the architecture of digital spaces and networks regulates behavior); Joel R. Reidenberg, *Lex Informatica: The Formulation of Information Policy Rules Through Technology*, 76 TEX. L. REV. 553 (1998) (arguing that lawmakers and regulators should take the regulatory function of digital architectures into account when formulating information policy).

18. *See, e.g.*, JULIE C. INNESS, PRIVACY, INTIMACY, AND ISOLATION (1992); Judith Wagner DeCew, *The Scope of Privacy in Law and Ethics*, 5 LAW & PHIL. 145 (1986).

the extent that it is grounded in the nexus between protected activity and protected space.[19]

One might argue that a claim right to noninterference defines a liberty interest, not a privacy interest.[20] But this objection misses the point. Privacy and liberty interests may overlap, but that does not render privacy claims identical to liberty claims. The interest in noninterference with behaviors of intellectual consumption within private spaces is not "simply" a matter of (negative) liberty, but also and more fundamentally a matter of the ability to exert positive control over an activity fundamental to self-definition.[21] Technologies of direct constraint shape individual practices of intellectual consumption in ways that shift the locus of choice about those practices away from the individual. At least when such practices occur within private spaces, then, these technologies implicate privacy interests. More specifically, the conjunction of constitutive activity and protected place generates a privacy interest in the ability to pursue the activity free from (at least some degree of) constraint.

---

19. Thus, for example, my argument would not necessarily support a claimed privacy interest in gaining physical access to Borders at three in the morning. It is worth reiterating, however, that the home is not the only sort of space in which this interest in freedom from constraint exists. For further discussion of this point, see *infra* Part III.A.1.a). Note also that I do not intend to suggest that individuals have no decisional autonomy interests whatsoever in intellectual activity outside private spaces; that is a separate question.

20. *See, e.g.*, Gavison, *supra* note 2, at 438-39. For other scholars who are generally skeptical of privacy claims, the failure of privacy scholars to agree on a single definition of privacy signals a fundamental weakness in the notion of "privacy" as an independent philosophical concept. *See, e.g.*, Thomson, *supra* note 6. Arguably, though, recourse to multiple, sometimes overlapping, definitions of privacy is entirely reasonable and does not weaken the case that privacy interests exist. *See, e.g.*, Daniel J. Solove, *Conceptualizing Privacy*, 90 CAL. L. REV. 1087 (2002) (suggesting a pragmatic, family-of-concepts approach to privacy). That is the general view that I adopt here. The virtues and vices of definitional consistency are subjects for another article. Since this Article addresses privacy in the particular context of intellectual property enforcement, however, I cannot resist noting that recourse to multiple, sometimes overlapping, definitions of "property" and its entailments does not seem to trouble some of the same commentators nearly as much.

21. *Cf.* DeCew, *supra* note 18, at 165:

> [C]ertain personal decisions regarding one's basic lifestyle . . . should be viewed as liberty cases in view of their concern over decision-making *power*, whereas privacy is at stake because of the *nature* of the decision . . . . [I]t is no criticism or conflation of concepts to say that an act can be both a theft and a trespass. Similarly, acknowledging that in some cases there is both an invasion of privacy and a violation of liberty need not confuse those concepts.

One also might object that defining intellectual privacy to encompass the absence of constraint makes every product design decision a privacy problem, and that this result does not square with the realities of the competitive marketplace. According to this view, DRM technologies of constraint, like any other new consumer product feature, simply create for users new realities around which to exercise (fewer remaining) choices. This, though, presumes that "product design" results from a confluence of neutral/technical factors exogenous to social policy. Exactly the opposite is true. Product design reflects social as well as "technical" values—or perhaps more precisely, technical considerations cannot help but reflect social ones.[22] For an example, one need look no farther than DRM technologies themselves; design for maximum constraint reflects commercial and (anti)competitive objectives.

To the extent that product design is inherently a social enterprise, there is no reason to say that privacy does not "belong" in the calculus of factors that inform and constrain design. To the contrary, if intellectual privacy is an important human value and product design implicates that value, then product design is a privacy issue, and rightly so.[23] Sometimes privacy values will receive only partial accommodation; one cannot say that privacy is the only relevant design consideration. But one can articulate as an explicit norm of the design process the goal of minimizing privacy-invasive constraints. As I discuss in greater detail in Part IV, injecting this norm into the DRM design process might produce DRM technologies that look substantially different.

2. Monitoring

Other DRM technologies are designed to report back to the information provider on the activities of individual users. Such reporting may occur in conjunction with a pay-per-use arrangement for access to the work, or it may occur independently of payment terms. For example, monitoring functionality might be designed to collect data about use of the work that might reveal user preferences for particular types of content.[24] Monitoring

22. *See, e.g.*, WIEBE E. BIJKER, OF BICYCLES, BAKELITES, AND BULBS: TOWARD A THEORY OF SOCIOTECHNICAL CHANGE (1995); DONALD MACKENZIE, KNOWING MACHINES: ESSAYS ON TECHNICAL CHANGE (W.E. Bijker et al. eds. 1996); LANGDON WINNER, THE WHALE AND THE REACTOR: A SEARCH FOR LIMITS IN AN AGE OF HIGH TECHNOLOGY (1986).

23. The point extends, as well, to other privacy values, but that is not my focus here.

24. For examples of this type of monitoring functionality, see Specht v. Netscape Communications Corp., 306 F.3d 17 (2d Cir. 2002) (involving alleged invasion of privacy by use of browser "plug-in" to monitor online activity); *In re* RealNetworks, Inc., Privacy Litig., No. 00-1366, 2000 WL 631341 (N.D. Ill. May 8, 2000) (involving privacy

also can be used to determine information about related products, such as the presence of non-copy-protected MP3 files on the user's hard drive or the other computer programs a user is running in conjunction with a licensed program.[25]

DRM technologies that monitor user behavior create records of intellectual consumption. Indirectly, then, they create records of intellectual exploration, one of the most personal and private of activities. They also create records of behavior within private spaces, spaces within which one might reasonably expect that one's behavior is not subject to observation. These technologies fall straightforwardly within conventional understandings of privacy invasion. Gathering information about intellectual consumption renders intellectual preferences accessible, both to the information provider and to third parties that might purchase it or invoke legal process to compel its production. And to the extent that behaviors within private spaces become accessible, or potentially accessible, to the outside world, the individual has lost a portion of the privacy that seclusion ought to guarantee.

Much of this record-keeping activity is conducted automatically, without the direct involvement of a human observer or controller, but the fact of automation does not necessarily neutralize the threat to privacy interests. The relevant question, instead, is whether information about intellectual consumption is gathered and stored in a form that is both personally-identifiable and potentially accessible to others.[26] If the information exists in such a form, it is subject to disclosure or compelled production. Absent stringent privacy protections (of which more later), the threat of disclosure may chill intellectual exploration, and therefore compromise intellectual privacy interests.

---

claims regarding media player software that monitored and stored information about users' electronic communications); *cf. In re* Pharmatrak, Inc., Privacy Litig., 220 F. Supp. 2d 4 (D. Mass. 2002) (discussing use of "cookies" to collect personal information about web site users); *In re* DoubleClick, Inc. Privacy Litig., 154 F. Supp. 2d 497 (S.D.N.Y. 2001) (same); John Borland, *A Secret War: Spike in "Spyware" Accelerates Arms Race*, CNET NEWS.COM (Feb. 24, 2003), *at* http://news.com.com/2102-1023-985524.html (describing recent developments in use of web-based technologies to gather information about habits and preferences of Internet users).

25. *See* Mark Prigg & Avril Williams, *Spies Behind Your Screen*, TIMES (London), Aug. 6, 2000, *available at* 2000 WL 23215148; *see also* Borland, *supra* note 24 (describing wide variety of information discoverable through use of monitoring software); Robert Lemos, *Trust or Treachery? Security Technologies Could Backfire Against Consumers*, CNET NEWS.COM (Nov. 7, 2002), *at* http://news.com.com/2102-1001-964628.html.

26. As noted in Part IV *infra*, techniques for aggregating user data for marketing purposes may avoid or substantially mitigate this privacy threat.

DRM monitoring technologies also can have second-order privacy effects. Specifically, data gathered through monitoring can later be used to generate detailed profiles of users' revealed intellectual preferences. The information provider can use the resulting profiles to market additional information goods to users, or can sell it to third parties who may use it for a wide variety of other purposes.[27] DRM monitoring technologies do not uniquely enable profiling, or even intellectual profiling; without any information about usage patterns, an information provider can construct a reasonably detailed profile of intellectual preferences and subject matter interests based solely on the information generated by initial purchase records. Nonetheless, the use of data gathered via DRM monitoring to "enhance" existing profiles renders those profiles more comprehensive, and thus potentially more invasive from the user's perspective.

3. Self-Help

Direct restriction protocols can be designed to encode penalties as well as disabilities. For example, a DRM system could be designed to disable access to a work upon detecting an attempt at unauthorized use.[28] Such "self-help" technologies—so named because they are designed to obviate recourse to legal enforcement procedures—might be directed and controlled externally upon detection of the prohibited activity. This type of functionality would need to be implemented in tandem with some sort of monitoring functionality. Self-help technologies also might operate automatically upon internal detection of a triggering activity, without communication with any external system or controller. The extent to which either type of self-help functionality should be permissible as a matter of contract law has been the subject of an ongoing dispute,[29] but there appear to be no technical barriers to their implementation.

DRM self-help technologies present a special case of the constraint problem, and potentially a special case of the monitoring problem as well.

---

27. For good discussions of profiling and its uses, see OSCAR H. GANDY, JR., THE PANOPTIC SORT: A POLITICAL ECONOMY OF PERSONAL INFORMATION (1993); Jeff Sovern, *Opting In, Opting Out, or No Options at All: The Fight for Control of Personal Information*, 74 WASH. L. REV. 1033 (1999).

28. *See, e.g.*, Chris Jay Hoofnagle, *Consumer Privacy in the E-Commerce Marketplace 2002*, 3 INTERNET L. & BUS. 812 (2002), *available at* http://www.epic.org/epic/staff/hoofnagle/ilbpaper.html (last visited May 5, 2003) (describing InTether's Point-to-Point system).

29. *See* UNIF. COMPUTER INFO. TRANSACTIONS ACT [hereinafter UCITA] 605(f), 816 cmt. 2 (amended 2002); UCITA 605(f), 816 cmt. 3 (amended 2001); UCITA 605, 815-16, (Draft 1999); U.C.C. 2B-715, reporter's note 3 (Draft Aug. 1, 1998); U.C.C. 2B-716 (Draft Apr. 15, 1998); U.C.C. 2B-716 (Draft Feb. 1998); *see also* Julie E. Cohen, *Copyright and the Jurisprudence of Self-Help*, 13 BERKELEY TECH. L.J. 1089 (1998).

For all of the reasons already discussed, I believe that it is analytically sound to conclude that both types of technologies have the potential significantly to diminish privacy in intellectual consumption. There remains the question whether the inclusion of self-help functionality adds anything distinct to the privacy dynamic.

The punitive quality of self-help implicates privacy interests in one way that technologies of direct constraint do not. The identification of a particular consumer as a target for self-help measures entails loss of the relative anonymity formerly enjoyed by that individual as one among many customers.[30] Here too, DRM technologies give the dynamics of enforcement a slightly different spin. Enforcement, like constraint and monitoring, can be activated without direct human agency; thus, it is conceivable that no human would ever know the specific identities of those singled out. Once again, though, conceptualizing loss of privacy in terms of *human* "attention" misses the distinctive sense in which the phenomenon of attention operates in the digital age. Attention and anonymity, or at least fungibility, may coexist. One can remain an anonymous customer and yet be singled out by a process of automated decisionmaking for consequences that one would not choose. Whether a human or a computer directed the decision, one's eBooks and MP3 files no longer "work," and no longer work as a result of actions taken privately. From the individual user's perspective, the consequences are the same regardless of whether a human or a computer made the final call to activate self-help measures.

It is worth noting, finally, that the deployment of DRM technologies of self-help, and more generally of constraint, also raises questions about the nature and function of the boundary between public and private spheres.[31] By inserting automatic enforcement functions into private spaces and activities, these technologies elide the difference between public/rule-governed behavior and private behavior that is far more loosely circumscribed by applicable rules and social norms. Some offenses, most notably crimes against persons, are so severe that they may justify such elision. In other cases, however, looseness of fit between public rules and private behavior serves valuable purposes. Where privacy enables individuals to avoid the more onerous aspects of social norms to which they may not

30. *See* Gavison, *supra* note 2, at 432-33 ("An individual always loses privacy when he becomes the subject of attention.").

31. "Public" and "private" are terms with multiple meanings. I use "private" here not to denote non-state activities, but simply to denote spaces not open to the general public and behaviors not intended for the general public, including private intellectual activities. I use "public" to denote conduct that occurs outside these realms.

fully subscribe, it promotes tolerance and pluralism.[32] Where the precise contours of legal rules are unclear, or the proper application of legal rules to particular facts is contested, privacy shields a range of experimentation with different behaviors that furthers the value-balancing goals of public policy. Highly restrictive DRM technologies do not permit this experimentation, and eliminate public policy and privacy alike from the calculus of infraction and enforcement. That these technologies, represent, at most, a novel form of distributed/decentralized authoritarianism seems cold comfort. Here again, privacy interests and liberty interests overlap, but are distinct. Privacy shields self-constitutive decisions and activities from interference, and protects liberty as well.[33]

* * *

Thus far, I have concentrated solely on identifying and elaborating individual interests in intellectual privacy, without considering whether or how society should protect those interests. The discussion has, however, identified two possible points of entry for the project of protecting intellectual privacy. First, law might translate intellectual privacy interests into enforceable rights by providing legal claims and remedies for (at least some) invasions of those interests. Second, privacy values might be introduced into the design process for DRM technologies. The remainder of the Article explores these possibilities.

III. BUILDING INTELLECTUAL PRIVACY INTO LAW

Articulating legal principles for protecting the intellectual privacy interests implicated by DRM technologies is far more complicated than articulating the normative case for such protection. Normative theories are more supple than legal ones, which tend to move cautiously along well-trodden paths. Developing a legal theory of intellectual privacy for the information age requires an act of legal imagination. Because no single branch of legal doctrine supplies all of the elements necessary for effective protection of intellectual privacy, such a theory must synthesize elements from a variety of different legal traditions. It also must confront directly a problem that each of these doctrinal traditions has steadfastly avoided: determining what conditions should be necessary for an effective waiver of

32. *Cf.* James E. Fleming, *Securing Deliberative Autonomy*, 48 STAN. L. REV. 1 (1995) (elaborating the role of constitutionally protected privacy in securing a realm of "deliberative autonomy").

33. *See* DeCew, *supra* note 18, at 172; *supra* Part II.B.1. A more detailed exploration of the relationship(s) between architectural constraint, privacy, and freedom is beyond the scope of this Article.

intellectual privacy if protection for intellectual privacy is to be meaningful. At both stages, the theory must be justified as an act of legal imagination. That is to say, it should be possible to show (capitulating at least partially to law's inherent conservatism) that it at least does not differ too greatly from other such imaginative leaps.

A. Crafting Legal Privacy Standards for the Information Age

Many different strands of law bear to some degree on questions of intellectual privacy, but none is exactly developed to address the unique privacy problems created by DRM technologies. Several, however, have the potential to do so. The common law of privacy, with its emphasis on control over personal spaces, private facts, and commercialization of image, can be reconfigured for the digital age by drawing on the policy and normative frameworks embodied in other privacy-regarding areas of law. In addition, because many information goods are also consumer goods, a more explicitly regulatory approach to privacy-invasive DRM technologies, grounded in principles of consumer protection law, can significantly improve levels of protection for intellectual privacy.

1. The Common Law Privacy Torts

The initial theory of common law privacy protection articulated by Warren and Brandeis was fairly flexible: a general "right to be let alone."[34] The difficulty with this new right lay precisely in its generality and vagueness; without a more detailed specification, the right to be let alone could conceivably encompass almost any kind of unwanted attention. By the mid-twentieth century, aided by legal scholarship seeking to subdue Warren and Brandeis' unruly brainchild, the common law of privacy had congealed into four distinct torts.[35] The price of clarity, however, was stasis. Three of these torts—intrusion upon seclusion, appropriation of name or likeness, and public disclosure of private facts—are potentially applicable to the privacy problems created by DRM technologies, but all have remained firmly focused on the privacy problems of the predigital age. Yet each is potentially flexible enough to cover far more—if only courts become convinced that the expansion is warranted.

---

34. Samuel D. Warren & Louis D. Brandeis, *The Right to Privacy*, 4 HARV. L. REV. 193, 193 (1890).

35. *See* KEETON, *supra* note 14, at § 117 (describing torts of appropriation of name or likeness, intrusion upon seclusion, public disclosure of private facts, and public portrayal in a false light); RESTATEMENT (SECOND) OF TORTS § 652A (1977) (same); Prosser, *supra* note 14. The tort-based theory of publicity rights was not included in this group, but emerged later and has proved more adaptable. *See infra* Part III.A.1.b.

Current applications of the common law privacy torts do not readily encompass the sorts of incursions worked by DRM technologies. As noted in Part II, the tort of intrusion upon seclusion has targeted physical or audiovisual intrusions into private spaces.[36] No court has considered whether it similarly protects against the insertion of other kinds of sensors (e.g., DRM monitoring technologies), or sensors that report back to machines rather than to people, or technologies that drastically constrain behavior, but without reporting back. Each of these conclusions requires an additional step away from the traditional core of the tort. The fit between current conceptions of the other common law privacy torts and informational privacy concerns is equally imperfect. The tort of appropriation of name or likeness has focused primarily on misuse of proper names and pictorial images for advertising purposes. So far, when asked to apply this tort to the digital "likenesses" generated by profiling and data mining activities, courts have resisted.[37] The tort prohibiting public disclosure of private facts has generally been applied in cases involving publication of embarrassing sexual, health-related or financial information, not the sale of information about intellectual habits and preferences.[38] All three of

36. *See, e.g.*, Ass'n Servs., Inc. v. Smith, 549 S.E.2d 454, 459 (Ga. Ct. App. 2001) (holding that trespassing upon private property while conducting surveillance could constitute intrusion upon seclusion); Miller v. Brooks, 472 S.E.2d 350 (N.C. App. 1996) (holding that placing a video camera in plaintiff's bedroom and going through his mail could constitute intrusion upon seclusion); Clayton v. Richards, 47 S.W.3d 149 (Tex. App. 2001) (holding that placing a video camera in plaintiff's bedroom could constitute intrusion upon seclusion).

37. *See, e.g.*, Dwyer v. Am. Express Co., 652 N.E.2d 1351 (Ill. App. Ct. 1995) (holding that credit card company did not appropriate cardholders' names or likenesses by renting lists of their names characterized by purchasing patterns); Avrahami v. U.S. News & World Report, Inc., No. 96-203, slip op. at 6-7 (Va. Cir. Ct. June 13, 1996) (holding that media company did not appropriate customer's name or likeness by selling information about him). This resistance is particularly incongruous in light of the fact that courts have shown relatively little restraint in expanding celebrity rights of publicity to cover new digital manifestations. *See infra* Part III.A.1.b.

38. *See, e.g.*, Bratt v. IBM Corp., 467 N.E.2d 126 (Mass. 1984) (allowing claim for publication of private facts where results of employee's psychiatric tests were disclosed to co-workers and supervisors); Doe v. Mills, 536 N.W.2d 824 (Mich. Ct. App. 1995) (holding that plaintiff stated prima facie case of publication of private facts where anti-abortion protesters displayed her name outside an abortion clinic); Y.G. v. Jewish Hosp., 795 S.W.2d 488 (Mo. Ct. App. 1990) (holding that plaintiffs stated claim for publication of private facts where information about their participation in hospital in vitro fertilization program was televised). There are some signs, however, of increasing judicial receptiveness to application of this tort to commercial profiling involving information perceived as especially sensitive. *See* Weld v. CVS Pharmacy, Inc., No. Civ. A. 98-0897F, slip op. at 1 (Mass. Super. Ct. June 29, 1999) (denying defense motion for summary judgment on claim that it invaded plaintiffs' privacy by selling information about their

these torts, however, are capable of a broader and more sensitive application.

Conceptual support for expansion of the common law privacy torts to cover electronic intrusion and monitoring can be found in policies derived from two bodies of law more finely attuned to intellectual privacy concerns: constitutional privacy law and copyright law. Compared with common law privacy rights, constitutional privacy rights manifest far greater concern with intellectual privacy. The drafters of the Constitution were concerned with safeguards against government overreaching, and so constitutional protections for intellectual privacy have no direct application to the practices of private information providers. These protections are instructive nonetheless, for they reflect a set of values that our legal culture has identified as important and worth preserving. In particular, fourth and first amendment law supply principles designed to protect the spatial and informational attributes of intellectual privacy. Copyright law, meanwhile, implicitly presumes a degree of "breathing space," and of anonymity, for users of intellectual goods. In different ways, then, each body of law intersects with and operationalizes aspects of the normative framework developed in Part II.

a) DRM Technologies and Intrusion Upon Seclusion

Application of the intrusion tort to DRM technologies finds parallels in a rapidly growing body of law that addresses the fourth amendment status of various types of remote information gathering. The federal courts have concluded that at least sometimes, disembodied intrusions by remote data sensors invade privacy rights protected by the fourth amendment. Most recently, in *Kyllo v. United States*,[39] the Court held that extraction of heat signature information emanating from the defendant's home constituted a search, and required a warrant. In particular, the majority focused on the fact that the extraction technology was "not in general public use" and the fact that it enabled access to "details of the home that would previously have been unknowable without physical intrusion."[40] *Kyllo* does not address whether reporting back to a machine should count, yet on the

medical prescriptions); *see also* Bodah v. Lakeville Motor Express, Inc., 649 N.W.2d 859 (Minn. Ct. App. 2002) (holding that employees stated a claim for publication of private facts where employer transmitted their social security numbers to third parties).

39. 533 U.S. 27 (2001); *see also* United States v. Karo, 468 U.S. 705 (1984) (holding that use of an electronic beeper to track goods taken into a private residence constituted a search within the meaning of the Fourth Amendment). *But see* Smith v. Maryland, 442 U.S. 735 (1979) (holding that use of pen register to record telephone numbers dialed from a private home was not an unreasonable search).

40. *Kyllo*, 533 U.S. at 40.

Court's reasoning there seems no reason why it should not. The search consists of the act of extraction, not what may or may not follow it.

Important questions remain about the scope of fourth amendment protection against virtual intrusion. First, it remains unclear whether the strong privacy protection specified by the *Kyllo* Court is to be limited specifically to the home.[41] The majority's brand of originalism supports this interpretation,[42] but other approaches to constitutional interpretation might not.[43] In delineating the legally cognizable scope of intellectual privacy interests, this is a particularly important question. Homes are but one kind of private space, and perhaps not even the most significant where intellectual activity is concerned.[44] Arguably, one's desktop or laptop computer, personal data assistant, or portable media player sits at the center of the zone of intellectual privacy to which one is entitled, regardless of where in physical space it happens to be located.[45]

Second, the "general public use" and "previously unknowable" inquiries frame a difficult problem that pervades both constitutional and common law privacy jurisprudence. In the common law context, these inquiries translate into the requirement that the intrusion be "offensive to the reasonable person."[46] Like the "reasonable expectation of privacy" standard on which they build, all of these standards render privacy a moving target. Eventually, the courts will need to confront the fact that the ultimate consequence of such an approach may be no privacy at all.

In resolving both of these questions, it is important to note—both for fourth amendment purposes and for insight into the lessons that the common law of privacy should draw from its constitutional cousin—that the text of the fourth amendment places intellectual privacy front and center.

---

41. *See* Andrew Riggs Dunlap, Note, *Fixing the Fourth Amendment with Trade Secret Law: A Response to* Kyllo v. United States, 90 GEO. L.J. 2175, 2190 (2002).

42. The Court grounded its holding in "that degree of privacy that existed when the Fourth Amendment was adopted." *Kyllo*, 533 U.S. at 34.

43. *See, e.g.*, LESSIG, *supra* note 17; Lawrence Lessig, *Fidelity in Translation*, 71 TEX. L. REV. 1165 (1993); Michael Adler, Note, *Cyberspace, General Searches, and Digital Contraband: The Fourth Amendment and the Net-Wide Search*, 105 YALE L.J. 1093, 1114 (1996); Dunlap, *supra* note 41.

44. *See* Dunlap, *supra* note 41, at 2187 ("Modern America is defined by the mobility of its people and their information.").

45. Perhaps for this reason, government agents appear to believe that a warrant is required for searches of these items. *See* United States v. Runyan, 290 F.3d 223, 236 (5th Cir. 2002); United States v. Triumph Capital Group, Inc., 211 F.R.D. 31, 39 (D. Conn. 2002). *But cf.* Aronson v. Sprint Spectrum, L.P., 767 A.2d 564 (Pa. Super. Ct. 2001) (holding that telecommunications company did not intrude upon customers' seclusion by allowing third parties to access their account information).

46. KEETON ET AL., *supra* note 14, at § 117

The amendment extends protection against warrantless search and seizure not simply to the home, but also to individuals' "papers and effects."[47] If individuals have no recourse against warrantless remote extraction of information from digital analogues to these items, wherever in physical space they may be located and however "ordinary" the technology used, then this protection stands to lose much of its meaning.[48] So too, on the common law side, if widespread efforts to enshrine a new technology as a commercial standard can displace privacy rights.[49] In the particular context of DRM, the deeply personal and private nature of intellectual activity provides relatively firm grounding for the conclusion that expecting adequate protection for intellectual privacy is reasonable regardless of the number of ways in which technologies for delivery of intellectual goods can be designed to diminish privacy.

The Fourth Amendment's greater sensitivity to the intersections between spatial privacy and intellectual privacy is an important guidepost for courts in common law intrusion cases to follow, if they choose. Even fourth amendment jurisprudence, however, provides relatively little assistance in assessing whether direct constraints, without any reporting back, invade a legally protectable privacy interest. By its own terms, the fourth amendment cannot even reach this question. Whether or not they are considered to invade privacy, such constraints cannot constitute a "search."

The argument that effective privacy protection should include control over the spaces of intellectual consumption finds support, instead, within both the substantive provisions and the overall structure of copyright law. The fair use doctrine, which sanctions certain acts of private copying, shields a range of actions that users might take in private spaces, including time- and space-shifting of copies, loading and reloading of digital files, and manipulation of digital content.[50] The first sale doctrine, which establishes the right to dispose of one's copy of a work without any obligation

---

47. U.S. CONST. amend. IV; *see also* Dunlap, *supra* note 41, at 2190-93.

48. *See* Adler, *supra* note 43; Dunlap, *supra* note 41, at 2190 ("Theoretically, then, if one could pick up a thermal imager at Wal-Mart for a reasonable cost, it would not create concern under [*Kyllo*].").

49. For more detailed discussion of this point, see Julie E. Cohen, *Privacy, Ideology, and Technology: A Response to Jeffrey Rosen*, 89 GEO. L.J. 2029, 2033 (2001).

50. 17 U.S.C. § 107 (2000); *see also* Sony Corp. v. Universal City Studios, Inc., 464 U.S. 417 (1984); Mattel, Inc. v. Pitt, 229 F. Supp. 2d 315, 321-24 (S.D.N.Y. 2002); *cf.* Recording Indus. Ass'n (RIAA) v. Diamond Multimedia Sys., 180 F.3d 1072, 1079 (9th Cir. 1999) (holding that digital music player designed to allow space-shifting, but not further copying, of digital music files was not covered by the Audio Home Recording Act's royalty and copy-protection requirements, and that this result was consistent with the AHRA's exemption for personal noncommercial copying).

to seek the copyright owner's approval,[51] similarly rests on the belief that a copyright owner has no cognizable interest in a broad range of post-purchase user activities or in the spaces where they occur. More broadly, because copyright law does not give copyright owners the exclusive right to control all uses of their copyrighted works, it implicitly reserves to users the right to engage in conduct not encompassed by the statute.[52] Copyright does not, for example, encompass such acts as reading a copy of a book, viewing a copy of a movie, or listening to a copy of a musical recording that one owns; not coincidentally, these are all acts that ordinarily occur within private spaces.

It may be argued that the Digital Millennium Copyright Act's (DMCA) protections for DRM technologies threaten to change rather substantially, and as a matter of federal law, the degree of informational and spatial privacy to which users of intellectual goods are entitled. In fact, the language of the DMCA supports the opposite conclusion: Congress did not intend the DMCA to negate the intellectual privacy of information consumers. An exception to the DMCA's anti-circumvention provision authorizes users of copyrighted works to circumvent technical measures capable of collecting or disseminating information about their "online activities" if those measures are undisclosed and do not provide an opt-out mechanism.[53] Under this provision, users appear free to subvert certain types of DRM monitoring. In addition, a special savings provision of the statute expressly preserves federal and state laws protecting individual privacy "in connection with the individual's use of the Internet."[54] The

51. 17 U.S.C. § 109(a).

52. In this respect, the fair use doctrine is poorly named. The term "fair use" tends to suggest that if some uses of copyrighted works are fair, then all other uses must be unfair. Fair use and other copyright limitations are not outer limits on permissible uses of copyrighted works and/or the things embodying them. They are simply outer limits on a copyright owner's statutory rights. Uses not covered by any of those rights, such as reading a copy of a book that one owns, are reserved to users whether or not the fair use doctrine would apply to them.

53. *See* 17 U.S.C. § 1201(i). Paul Schwartz has argued that these provisions should be understood, in part, as an attempt to stimulate the adoption of notice and opt-out norms for the online marketplace. *See* Paul M. Schwartz, *Internet Privacy and the State*, 32 CONN. L. REV. 815, 848-50 (2000).

54. 17 U.S.C. § 1205 ("Nothing in this chapter abrogates, diminishes, or weakens the provisions of, nor provides any defense or element of mitigation in a criminal prosecution or civil action under, any Federal or State law that prevents the violation of the privacy of an individual in connection with the individual's use of the Internet."). This provision is probably best interpreted as preserving information providers' obligations under the federal Electronic Communications Privacy Act and analogous state laws; thus, for example, a software company caught monitoring customers' use of its e-mail program could not claim that the DMCA allows it to do so.

DMCA says nothing about its interaction with other federal or state privacy laws, just as it says nothing about its interaction with many other background rules of law, but that does not mean it negates them. (The DMCA says nothing about its interaction with the background law of contract, either.) That users are not authorized to circumvent a broader range of privacy-invasive measures does not mean that information providers have carte blanche to employ them. The most plausible explanation for the specific provisions relating to online activities is simply that interest groups brought these problems to the drafting committees' attention. The legislative history does not suggest that any of the relevant committees ever undertook a more thorough exploration of the privacy question.

In short, copyright law traditionally has honored a version of the public-private distinction that is extremely robust,[55] and the DMCA does not purport to reject that tradition. Whether a provider of digital information is honoring or abusing this distinction should inform application of the common law intrusion tort, even to (at least some) DRM technologies that simply impose direct constraints on user behavior. From a copyright perspective the difference between reporting back and simple constraint is less relevant than the difference between public exploitation and private consumption. When deciding whether particular DRM constraints rise to the level of an actionable intrusion, courts should take this perspective into account.

b) DRM Technologies, "Likenesses," and "Private Facts"

Application of the appropriation and "private facts" torts to DRM monitoring technologies finds parallels in first amendment jurisprudence touching on intellectual privacy. First amendment cases involving the compelled disclosure of reading and viewing habits find intellectual activity quintessentially private because of the chilling effect on private expressive and political activity that might result from compelled disclosure of opinions and associations.[56] The chill may diminish when private compul-

---

55. For other perspectives on the public-private distinction within copyright law, see PAUL GOLDSTEIN, COPYRIGHT'S HIGHWAY: FROM GUTENBERG TO THE CELESTIAL JUKEBOX 28-30, 216-24(1994), acknowledging the distinction but arguing that copyright should extend its reach into private spaces, and JESSICA LITMAN, DIGITAL COPYRIGHT 194-95 (2001), arguing that copyright rules should conform more nearly to user expectations.

56. *See* Denver Area Educ. Telecomm. Consortium, Inc. v. FCC, 518 U.S. 727, 751-66 (1996); Stanley v. Georgia, 394 U.S. 557, 563-66 (1969); Schneider v. Smith, 390 U.S. 17, 24-25 (1968); Lamont v. Postmaster Gen., 381 U.S. 301, 307 (1965); Fabulous Assoc., Inc. v. Pa. Pub. Util. Comm'n, 896 F.2d 780, 785 (3d Cir. 1990); *see also* Gibson v. Fla. Legislative Investigation Comm., 372 U.S. 539, 544 (1963); Bates v. City of Little

sion replaces state compulsion, but it does not disappear. In the age of distributed databases, the pertinent fact is that a record of the activity exists, and may be acquired and used by either state or private parties.[57]

On similar reasoning, both the private facts and appropriation torts should encompass the sale, rental, or trading of information about patterns of intellectual consumption. Arguably, the harms resulting from disclosure of private facts relating to intellectual activities and preferences are at least as great as those resulting from disclosure of information about sexual activities and preferences, since it is the former rather than the latter upon which a democratic society relies to constitute its citizens. And if a profile of intellectual activities and preferences can chill expressive and associative conduct, it is hard to see why it should not be deemed a "likeness"—whether flattering or unflattering is beside the point—of the individual to whom it refers. Nor is it relevant that this sort of consumer profiling activity typically does not involve general publication of the offending information. Both torts also have been recognized in cases involving more limited publication.[58] For the private facts tort, the touchstone is the disclosure and the injury it causes; for the appropriation tort, it is the unauthorized commercial use. In neither case does the injury depend on general publication, but rather on the nature of the information and the identities of the recipients.[59]

Rock, 361 U.S. 516, 523-24 (1960); NAACP v. Alabama *ex rel.* Patterson, 357 U.S. 449, 460-62 (1958). *See generally* Cohen, *A Right to Read Anonymously*, *supra* note 2, at 1008-15 (analyzing the cases and arguing that arguing that they implicitly recognize a right of anonymity for readers, viewers, and listeners).

57. *See In re* Grand Jury Subpoena to Kramerbooks & Afterwords, Inc., 26 Med. L. Rptr. 1599, 1600 (D.D.C. 1998); Tattered Cover, Inc. v. City of Thornton, 44 P.3d 1044, 1047 (Colo. 2002).

58. Among the recent information privacy cases discussing this point are *Bodah v. Lakeville Motor Express, Inc*., 649 N.W.2d 859 (Minn. Ct. App. 2002), and *Weld v. CVS Pharmacy, Inc.*, No. Civ. A. 98-0897F, 1999 WL 494114 (Mass. Super. Ct. June 28, 1999).

59. Notwithstanding that first amendment values support extension of the appropriation and private facts torts to protect intellectual privacy, first amendment principles also limit the reach of both torts. Although the exact location of the first amendment boundary is a matter of some dispute, see, for example, Cohen, *Examined Lives*, *supra* note 2; Pamela Samuelson, *Privacy as Intellectual Property?*, 52 STAN. L. REV. 1125 (2000); Paul M. Schwartz, *Free Speech vs. Information Privacy: Eugene Volokh's First Amendment Jurisprudence*, 52 STAN. L. REV. 1559 (2000); Eugene Volokh, *Freedom of Speech and Information Privacy: The Troubling Implications of a Right to Stop People From Speaking About You*, 52 STAN. L. REV. 1049 (2000), it is not my intent to question its existence. It is worth noting, however, that precisely because of first amendment limitations on the scope of information privacy protection, one might legitimately conclude that limited disclosures of information about intellectual activities and preferences between

Further support for expansion of the appropriation tort to encompass transactional identity comes, paradoxically, from privacy's commercial *doppelganger*, the common law right of publicity. Like the privacy tort of unauthorized appropriation, rights of publicity protect against unauthorized appropriation of names and likenesses. Rights of publicity typically are invoked to protect commercially valuable likenesses, while rights of privacy are not, but both theories seek to reserve control over commercial exploitation of identity to the individual with whom that identity is associated. Unlike courts hearing privacy cases, courts in publicity cases have generously construed the concept of "likeness," extending protection to any attribute of personality that can reasonably be identified as belonging to the plaintiff.[60] Courts and commentators justify this expansion with reference to both the increasing value of (celebrity) identity and the many forms that identity can assume in the age of mass culture and advertising.[61] If it is true that manifestations of identity have become increasingly protean in the information age, there seems to be no good reason why the common law of privacy should not also recognize protectable attributes of identity in commercial profiles. Indeed, the case for such protection is far stronger than in the publicity context; actual data about one's own transac-

---

parties intent on exploiting that information for commercial or prosecutorial benefit are more troubling than general/journalistic publication of the information.

60. *See, e.g.*, Waits v. Frito-Lay, Inc., 978 F.2d 1093, 1098-1100 (9th Cir. 1992) (imitation of singer's distinctive voice and singing style); White v. Samsung Elecs. Am., 971 F.2d 1395 (9th Cir. 1992) (game show hostess's gown and game show setting), *petition for reh'g and reh'g en banc denied*, 989 F.2d 1512 (9th Cir.), *cert. denied*, 508 U.S. 951 (1993); Midler v. Ford Motor Co., 849 F.2d 460, 463-64 (9th Cir. 1988) (imitation of singer's distinctive voice and singing style); Carson v. Here's Johnny Portable Toilets, Inc., 698 F.2d 831, 836-37 (6th Cir. 1983) (talk show host's "trademark" slogan); Motschenbacher v. R.J. Reynolds Tobacco Co., 498 F.2d 821, 827 (9th Cir. 1974) (race car driver's distinctively decorated car).

61. *See, e.g.*, Zacchini v. Scripps-Howard Broad. Co., 433 U.S. 562 (1977); Carissa Byrne Hessick, *The Right of Publicity in Digitally Produced Images: How the First Amendment Is Being Used to Pick Celebrities' Pockets*, 10 UCLA ENT. L. REV. 1 (2002); Roberta Rosenthal Kwall, *Fame*, 73 IND. L.J. 1 (1997); *see also* Jennifer L. Carpenter, *Internet Publication: The Case for an Expanded Right of Publicity for Non-Celebrities*, 6 VA. J.L. & TECH. 3 (2001) (arguing that private individuals also should enjoy rights of publicity in certain circumstances). Many commentators, however, argue that the unchecked expansion of publicity rights threatens other important public values, including freedom of expression and cultural diversity, and that the arguments advanced to support this expansion do not adequately answer these concerns. *See, e.g.*, Michael Madow, *Private Ownership of Public Image: Popular Culture and Publicity Rights*, 81 CAL. L. REV. 125 (1993); Diane Leenheer Zimmerman, *Fitting Publicity Rights into Intellectual Property and Free Speech Theory: Sam, You Made the Pants Too Long!*, 10 J. ART & ENT. L. & POL'Y 283 (2000).

tional history and preferences are far more directly bound up with identity than mere allusions intended to trigger some mental association in others.

Finally, the same copyright rules that create a presumption of spatial privacy also provide strong implicit support for informational privacy claims directed toward exploitation of the information gained from DRM monitoring. In particular, the fair use doctrine supports a strong presumption of anonymity around privileged uses. The functions and benefits of anonymity are clearest in the case of fair use. Fair use privileges a variety of activities that are deemed socially valuable, but to which private copyright holders might object.[62] Anonymity permits these activities to go forward, and allows fair users to decide later whether to reveal their identities when releasing their work. In other cases, the costs and delay involved in seeking permission might strike the would-be fair user as prohibitive, even if the overall social value resulting from the use would outweigh these costs.[63] Having to seek permission from the copyright holder ex ante would chill both types of uses; anonymity for fair users mitigates the twin problems of private censorship and high transaction costs, and allows society to receive the benefit of many controversial and/or spontaneous uses that otherwise would not occur.[64]

* * *

Synthesis of the intrusion, appropriation, and private facts torts with these insights derived from conceptually related areas of law would yield more expansive conceptions of actionable intrusion, appropriable identity, and sensitive personal information. This result is broadly consistent with

---

62. Examples of such activities include criticism, for example, *New Era Publ'ns Int'l v. Carol Publ'g Group*, 904 F.2d 152 (2d Cir. 1990), parody, for example, *Campbell v. Acuff-Rose Music, Inc.*, 510 U.S. 569 (1994), and *Suntrust Bank v. Houghton Mifflin Co.*, 268 F.3d 1257 (11th Cir. 2001), and the reverse engineering of computer software to achieve interoperability, for example, *Sony Computer Entm't, Inc. v. Connectix Corp.*, 203 F.3d 596 (9th Cir. 2000), and *Sega Enter., Ltd. v. Accolade, Inc.*, 977 F.2d 1510 (9th Cir. 1992).

63. *See* Julie E. Cohen, Lochner *in Cyberspace: The New Economic Orthodoxy of "Rights Management"*, 97 MICH. L. REV. 462 (1998); Lydia Pallas Loren, *Redefining the Market Failure Approach to Fair Use in an Era of Copyright Permission Systems*, 5 J. INTELL. PROP. L. 1 (1997); *cf.* Mark A. Lemley, *The Economics of Improvement in Intellectual Property Law*, 75 TEX. L. REV. 989 (1997). Examples of such activities include technical innovation in the design of search engines, for example, *Kelly v. Arriba Soft Corp.*, 280 F.3d 934, 942 (9th Cir. 2002), the design of consumer electronic equipment that facilitates both infringing and non-infringing uses of copyrighted content, for example, *Sony Corp. v. Universal City Studios, Inc.*, 464 U.S. 417 (1984), and reverse engineering again.

64. *See* Dan L. Burk & Julie E. Cohen, *Fair Use Infrastructure for Rights Management Systems*, 15 HARV. J.L. & TECH. 41, 60 (2001).

the normative model of privacy developed in Part II, which focuses on control of access to self and insulation for constitutive activities. It is also broadly consistent with the core policies underlying each tort: to preserve, respectively, individual control of space, identity, and "face."

Why, though, should the common law of privacy make these leaps? For all the ingrained conservatism of the common law method, recognizing and responding to changing circumstances by redefining legally cognizable injury and responsibility are central functions of the courts. Many legal rules that we take for granted today simply did not exist forty or fifty years ago. One example is the law of strict products liability, under which an injured consumer may recover damages directly from the manufacturer of a defective product even if there is no privity of contract.[65] Another is the law of sexual harassment, which recognizes that sex-based hazing in the workplace can amount to discrimination in violation of federal law.[66] In each context, the courts gradually came to recognize that new forms of injury resulting from changed marketplace realities warranted new modes of redress.

In a similar fashion, courts can and should respond to new forms of injury enabled by the rise of digital network communications and the attendant transformations of commerce in information. In copyright circles, this point is hardly novel, but lawmakers and courts have focused their attention largely on new sources of injury to information providers.[67] As these historical examples suggest, it is appropriate to focus, as well, on new sources of injury to information users, and doing so will not bring commerce in information screeching to a halt. The project of transforming existing doctrine to accommodate the unprecedented is itself firmly rooted in precedent.

There is, however, one major obstacle to the development of robust common law standards of intellectual privacy. Traditionally, common law privacy protections may be waived. As long as the contract is otherwise enforceable, one may consent to audio- or videotaping of the activities inside one's home, or to commercial exploitation of one's name or likeness,

---

65. *See* Escola v. Coca-Cola Bottling Co., 150 P.2d 436, 461 (Cal. 1944) (Traynor, J., concurring); Sheward v. Virtue, 126 P.2d 345 (Cal. 1942); State Farm Mut. Auto. Ins. Co. v. Anderson-Weber, Inc., 110 N.W.2d 449, 455 (Iowa 1961); Carter v. Yardley & Co., 64 N.E.2d 693, 695-96 (Mass. 1946); McCormack v. Hankscraft Co., 154 N.W.2d 488 (Minn. 1967); MacPherson v. Buick Motor Co., 111 N.E. 1050 (N.Y. 1916); Ritter v. Narragansett Elec. Co., 283 A.2d 255, 261 (R.I. 1971).

66. *See* Meritor Sav. Bank FSB v. Vinson, 477 U.S. 57 (1986); Bundy v. Jackson, 641 F.2d 934 (D.C. Cir. 1981); Tomkins v. Pub. Serv. Elec. & Gas Co., 568 F.2d 1044 (3d Cir. 1977); Berkman v. City of New York, 580 F. Supp. 226 (E.D.N.Y. 1983).

67. *See* LITMAN, *supra* note 55.

or to publication of sensitive information about one's sexual habits. Because the privacy invasions effected by DRM technologies occur in the context of consensual commercial transactions, the mechanisms for establishing effective consent can easily be put in place.

Neither copyright law nor constitutional privacy law offers a clear way out here. Constitutional protections also can be waived. Copyright law, meanwhile, is silent about when parties may contract around the rights and limitations that it specifies. This silence has engendered an extensive scholarly debate about whether such contracts should be prohibited, under either a theory of preemption or one of misuse, as violating fundamental public policy.[68] Detailed consideration of those debates is outside the scope of this Article; for our purposes, the important point is that neither preemption nor misuse is well-suited to address the privacy problems stemming from DRM technologies. The fundamental public policy that both doctrines seek to preserve is the "copyright balance" between incentives and access. User privacy serves related purposes, and a decision striking down a particular contract provision might have the effect of promoting privacy, but privacy is not central to the incentives/access inquiry. For a specifically privacy-regarding theory of contract's limits, we must look elsewhere.

2. Consumer Protection Law and the Fair Information Practices

Although consumer protection law has not traditionally been viewed as a significant component of information policy in the U.S., that is changing. In an era in which mass-distributed information goods are increasingly bundled with lengthy, complex licenses, the connections between consumer protection and information policy can no longer be ignored. Although the issue of privacy in intellectual consumption has not yet received specific attention, both the Federal Trade Commission (FTC) and intellectual property scholars have begun to focus more closely on these connections.[69] Where privacy is concerned, judge-made law and consumer

---

68. *See, e.g.*, Mark A. Lemley, *Beyond Preemption: The Law and Policy of Intellectual Property Licensing*, 87 CAL. L. REV. 111 (1999); David Nimmer et al., *The Metamorphosis of Contract Into Expand*, 87 CAL. L. REV. 17 (1999); J.H. Reichman & Jonathan A. Franklin, *Privately Legislated Intellectual Property Rights: Reconciling Freedom of Contract with Public Good Uses of Information*, 147 U. PA. L. REV. 875 (1999); David A. Rice, *Public Goods, Private Contract, and Public Policy: Federal Preemption of Software License Prohibitions Against Reverse Engineering*, 53 U. PITT. L. REV. 543 (1992).

69. *See* U.S. FED. TRADE COMM'N, COMPETITION AND INTELLECTUAL PROPERTY LAW AND POLICY IN THE KNOWLEDGE-BASED ECONOMY, *at* http://www.ftc.gov/opp/intellect/index.htm (last modified Oct. 28, 2002) (listing press releases and hearing notices from February through November 2002); U.S. FEDERAL TRADE COMM'N, WAR-

protection regulation have complementary roles to play. While properly reformulated common law privacy torts can police the worst excesses of DRM, consumer protection law operating prospectively can set minimum standards of protection that all information providers must follow.

One advantage of a consumer protection approach to the terms of information access and use is that it allows policymakers to consider consumer welfare directly, rather than waiting for courts to parse out the implications of a statutory scheme (such as copyright) designed primarily to accomplish some other purpose. Whether this change in emphasis might translate into significant substantive protection for consumers depends on the prevailing standard for consumer well-being. U.S. consumer protection law is not particularly well tailored to safeguard the intellectual privacy of information users. Like the common law privacy torts, however, it has the potential to be.

Consumer protection law in the U.S. has focused primarily, though not exclusively, on maximizing market-based indicia of consumer welfare. The FTC has jurisdiction to regulate "unfair or deceptive acts or practices in or affecting commerce."[70] In implementing this mandate, it has largely confined itself to policing deception, and has been reluctant to provide other sorts of protection to consumers who are adequately and accurately informed. Whatever the merits of this approach in other contexts, as an approach to privacy protection it is demonstrably inadequate. An extensive literature supports the conclusion that the idea of a well-functioning "market for privacy" is irremediably flawed.[71] In many transactions, retaining control of one's personal information simply is not an option. Even when it is, pervasive and likely incurable information problems prevent individuals from evaluating the relevant tradeoffs.[72] More fundamentally, privacy tradeoffs involve incommensurable values, and the dignitary values at stake in decisions about privacy arguably are not an appropriate subject

---

RANTY PROTECTION FOR HIGH-TECH PRODUCTS AND SERVICES, *at* http://www.ftc.gov/bcp/workshops/warranty/index.html (Oct. 26-27, 2000) (transcripts of hearings).

70. 15 U.S.C. § 45(a)(1) (2000).

71. *See, e.g.*, GANDY, *supra* note 27; Cohen, *Examined Lives*, *supra* note 2; A. Michael Froomkin, *Flood Control on the Information Ocean: Living with Anonymity, Digital Cash, and Distributed Databases*, 15 J.L. & COM. 395, 492 (1996); Paul M. Schwartz, *Privacy and Democracy in Cyberspace*, 52 VAND. L. REV. 1607 (1999) [hereinafter Schwartz, *Privacy and Democracy*]; Paul M. Schwartz, *Privacy and the Economics of Personal Health Care Information*, 76 TEX. L. REV. 1, 47-51 (1997) [hereinafter Schwartz, *Personal Health Care Information*]; Sovern, *supra* note 27.

72. *See* Cohen, *Examined Lives*, *supra* note 2, at 1397-99; Froomkin, *supra* note 71, at 492; Schwartz, *Personal Health Care Information*, *supra* note 71, at 47-51; Sovern, *supra* note 27, at 1052-94.

for market ordering.[73] For the reasons discussed in Part II.A, this argument is particularly strong where intellectual privacy is concerned. Under the Clinton Administration, the FTC called without success for federal legislation establishing stronger protection for online privacy.[74] If the FTC wishes to play a more effective role in safeguarding the intellectual privacy of information consumers, however, it can begin by rethinking its interpretation of its statutory mandate.

A somewhat more robust vision of information privacy protection is embodied in guidelines issued in 1980 by the Organization for Economic Cooperation and Development, which outlined a set of Fair Information Practices (FIPs) based on eight principles: collection limitation, data quality, purpose specification, use limitation, transparency of information collection practices, security of stored data, individual participation, and accountability.[75] Although the U.S. played an important role in developing these principles, the FIPs have never been fully incorporated into U.S. law. In part, this is the result of sustained resistance by the information and direct marketing industries. In part, it is because the proceduralist understanding of consumer protection already enshrined within FTC practice pairs more comfortably with a version of fair information practices based simply on notice and consent.[76] More faithful adherence to the FIPs would enhance the information privacy of users of copyrighted works and other information goods.[77] The FTC has taken some steps in that direction, but only partial steps and only pursuant to additional, narrowly defined statutory mandates.[78] Extending the full protection of the FIPs to all consumers

---

73. *See* Cohen, *Examined Lives*, *supra* note 2; Schwartz, *Privacy and Democracy*, *supra* note 71. For this reason, it may make sense to conclude that the law should protect (some aspects of) privacy even for individuals who would cheerfully trade it away. *See* Allen, *supra* note 2; Cohen, *Examined Lives*, *supra* note 2.

74. *See* U.S. FEDERAL TRADE COMMISSION, PRIVACY ONLINE: FAIR INFORMATION PRACTICES IN THE ELECTRONIC MARKETPLACE (2000).

75. *See* ORGANISATION FOR ECONOMIC CO-OPERATION AND DEVELOPMENT, RECOMMENDATION OF THE COUNCIL CONCERNING GUIDELINES GOVERNING THE PROTECTION OF PRIVACY AND TRANSBORDER FLOWS OF PERSONAL DATA, *in* OECD GUIDELINES ON THE PROTECTION OF PRIVACY AND TRANSBORDER FLOWS OF PERSONAL DATA 14-16 (Sept. 23, 1980), *available at* http://www1.oecd.org/publications/e-book/9302011E.PDF (last visited May 4, 2003) [hereinafter OECD GUIDELINES].

76. For discussion of this point, see Joel R. Reidenberg, *Restoring Americans' Privacy in Electronic Commerce*, 14 BERKELEY TECH. L.J. 771, 773-81 (1999).

77. It also would enhance the functioning of markets in personal information by ensuring that personal information is accurate and that data processing operations more completely internalize their costs.

78. *See* Privacy of Consumer Financial Information, 16 C.F.R. § 313 (2003); Children's Online Privacy Protection Rule, 16 C.F.R. § 312 (2003) (establishing rules governing online collection of personal information from children under 13); *see also* U.S.

is appropriate in an age in which personal profiling increasingly tracks not only purchases of durable goods but also private intellectual activities.

Even with more rigorous application of the FIPs, however, the problem of privacy in intellectual consumption is too complex to be resolved by data processing standards alone, for several reasons. First, the FIPs do not address spatial privacy, and so have nothing to say about the sorts of behavioral restrictions effected by DRM technologies.[79] Thus, even scrupulous adherence to the FIPs would not address all of the privacy concerns discussed in Part II. Second, even with respect to information privacy, the FIPs do not establish minimum substantive thresholds for privacy protection. At most, they are designed to facilitate informed contracting and meaningful quality control by individuals who are the subjects of data transactions. Finally and relatedly, the FIPs do not address important threshold questions of contract validity. That is, they say nothing about whether some privacy rights should be protected even against knowing waivers by informed consumers.

For consumer protection law to provide meaningful protection for intellectual privacy (or any other kind of privacy), the proceduralist standards embodied in the FIPs must be augmented by substantive privacy standards. Here the act of legal imagination consists in realizing that although the FTC has not traditionally involved itself in setting substantive standards of consumer protection, its mandate to address "unfair" trade practices is broad enough to encompass such a move.[80] Put differently, a

---

DEP'T OF COMM., SAFE HARBOR OVERVIEW, *in* SAFE HARBOR, *at* http://www.export.gov/safeharbor/sh_overview.html (last visited May 4, 2003) (establishing guidelines for U.S. companies that process personally identifying information relating to European Union citizens, and vesting enforcement authority with the FTC for most industries). To be fair, the FTC has been hampered to a degree by a sectoral approach to privacy regulation at the jurisdictional level. Jurisdiction to regulate in the area of medical privacy is vested in the Department of Health and Human Services, 42 U.S.C. § 1320c (2000), and jurisdiction to regulate in the area of telecommunications privacy is vested in the Federal Communications Commission, 47 U.S.C. § 227(c) (2000). Nonetheless, the FTC retains general authority to regulate unfair and deceptive practices over a wide range of goods and services.

79. Proposed legislation specifically authorizing the FTC to require accurate labeling of DRM technologies that directly constrain consumer behavior would address this omission, but again by providing only procedural protection to consumers. *See* Digital Consumer Right to Know Act, S. 692, 108th Cong. (2003); Digital Media Consumers' Rights Act of 2003, H.R. 107, 108th Cong. (2003).

80. The Federal Trade Commission's enabling statute defines an "unfair or deceptive act or practice" as one that "causes or is likely to cause substantial injury to consumers which is not reasonably avoidable by consumers themselves and not outweighed by countervailing benefits to consumers or to competition." 15 U.S.C. § 45(n) (2000). This definition is "not limited to those [practices] likely to have anticompetitive consequences

market-making conception of fairness is not the only possible definition of that term, nor is it the only sensible one. Where consumers cannot play on an equal footing with other market participants, it serves neither fairness nor markets to pretend they can.[81]

In the context of information privacy, one example of a substantive standard of fairness is the European Union's data processing directive, which delineates certain kinds of information as sensitive and allows member states to place them off limits.[82] Similarly, if intellectual profiling is deemed to create unacceptable risk of harm to consumers, one might envision a regulation setting limits on the collection, use, retention, and trading of such information.[83] In the context of spatial privacy, an example of substantive privacy protection might be a regulation prohibiting certain kinds of electronic self-help,[84] or preserving a limited degree of freedom to space-shift digital files. By establishing and enforcing these sorts of standards, consumer protection authorities can help to ensure that individuals retain meaningful control over both the spatial and informational dimensions of their own intellectual consumption.[85]

---

after the manner of the antitrust laws; nor [a]re unfair practices in commerce confined to purely competitive behavior." FTC v. Sperry & Hutchinson Co., 405 U.S. 233, 244 (1972). Instead, it gives the FTC authority to consider a broader range of "public values." *Id*.; *see also* Spiegel, Inc. v. FTC, 540 F.2d 287, 292-94 (7th Cir. 1976) (affirming FTC order requiring mail-order retailer to cease and desist from suing delinquent customers in its own home state, on the ground that invocation of the state's long-arm statute under those circumstances violated public policy).

81. Steven Hetcher has argued that the FTC's current stance toward online privacy, which emphasizes self-regulation via the adoption of privacy policies, constitutes an innovative attempt to extend jurisdiction over information privacy issues. Steven Hetcher, *The FTC as Internet Privacy Norm Entrepreneur*, 53 VAND. L. REV. 2041, 2046, 2056 (2000). According to Hetcher, the FTC's policy of "norm entrepreneurship" constitutes a logical response to the privacy problem given both the complexity of the problem and the difficulty of generating political consensus around the regulation of online conduct. *Id*. at 2052, 2055-58. I do not disagree with this assessment. My disagreement with the prevailing regulatory approach to privacy runs deeper, and is directed at the regulatory mindset that assumes that, when regulatory supervision is feasible, the optimal model is one that places primary reliance on markets.

82. *See* Council 95/46, 1995 O.J. (L 281) 31 (on the protection of individuals with regard to the processing of personal data and on the free movement of such data).

83. Such a regulation might be modeled on the Video Privacy Protection Act of 1988, 18 U.S.C. § 2710 (2000), or on state library privacy statutes. *See supra* note 4.

84. Such a regulation would also have the beneficial effect of resolving the ongoing debate among the drafters of UCITA. *See supra* note 29.

85. In addition, as I will discuss in Part IV, the law has an important role to play in ensuring that substantive protections for privacy are incorporated into the design of DRM technologies at the outset.

B. Contractual Waiver and Intellectual Privacy as Fundamental Public Policy

The single greatest obstacle to effective legal protection of privacy in intellectual consumption is not imperfect fit with the available legal theories, but the fact that each available theory gives way to contract in many, if not all, circumstances. Many believe that this deference to contract is entirely appropriate. They observe that, from the information provider's perspective, the greater power to withhold the transaction entirely logically includes the lesser power to impose conditions on the terms of access and use. From the individual user's perspective, these conditions may diminish privacy, but users remain free to accept or reject the terms offered to them. Indeed, advocates for market ordering of privacy rights argue that the right to contract away privacy interests is itself a good that consumers may desire. Privacy advocates have persuasively argued that the argument from contract is far too simplistic, and ignores both marketplace realities and important non-market considerations. Thus far, however, the law has failed to translate these challenges into a workable legal theory capable of displacing contract when threats to privacy reach unacceptable levels.

Some challenges to contractual ordering of privacy rights focus on imperfections that are likely to prevent market mechanisms from working smoothly. These challenges fall into two general categories. First are procedural challenges to the validity of waiver via online adhesion contracts. In the age of "clickwrap," however, defects relating to consent are easily cured by requiring the consumer to pass through a screen displaying license terms and to indicate assent to those terms after having had the opportunity to review them.[86] A second set of challenges based on market imperfections focuses on issues of market power. If a dominant vendor has

86. *See, e.g.*, ProCD, Inc. v. Zeidenberg, 86 F.3d 1447 (7th Cir. 1996); Caspi v. Microsoft Network LLC, 732 A.2d 528 (N.J. Super. Ct. App. Div. 1999); *see also* Specht v. Netscape Communications Corp., 150 F. Supp. 2d 585 (S.D.N.Y. 2001), *aff'd*, 306 F.3d 17 (2d Cir. 2002) (holding clickwrap terms unenforceable where transaction protocol did not include a review-and-assent procedure, but instead displayed license terms only to those users who scrolled past the download button and followed a link to terms posted elsewhere on the vendor's web site); Ticketmaster Corp. v. Tickets.com, Inc., 54 U.S.P.Q. 2d 1344 (C.D. Cal. 2000) (same). This is also the solution adopted by the drafters of UCITA. *See* UCITA § 209 (1999). This is not to make light of what commentators rightly identify as a paradigm shift in prevailing understandings of the sort of consent required to create a binding contract. *See, e.g.*, Margaret Jane Radin, *Humans, Computers, and Binding Commitment*, 75 IND. L.J. 1125 (2000). But that paradigm shift resulted from the rise of consumer mass markets decades ago. Technologies for indicating "consent" online simply underscore what we already know to be true: that in mass markets, the idea of a "meeting of minds" is little more than a pleasant fiction.

market power, it becomes harder to posit a meaningful level of competition to satisfy the full range of consumer preferences. But the conventional form of this inquiry looks only to the power of individual market participants, and not to the market power that results from widespread adoption of standard form terms.[87] As a result, this argument has weight only in monopoly markets, and therefore very little weight in most markets for online information goods.

Both types of argument from market imperfection, however, fit comfortably within a larger conceptual framework that presumes the rightness of market ordering if only some defect could be brought under control. Neither challenges the baseline presumption in favor of contractual ordering in properly functioning markets. As a result, each rapidly becomes mired in the details of this or that clickwrap procedure or market practice. The more fundamental question—whether market ordering of privacy rights makes sense at all—remains obscured. It is not terribly surprising, then, that these sorts of arguments have failed to generate the impetus for meaningful reform of the legal rules governing waiver of privacy rights.

Other challenges to contractual ordering of privacy rights step outside the market framework, and argue that even in perfectly functioning markets, contract would be ineffective to preserve privacy, or to do so fairly.[88] As discussed in Part III.A.2, some of these arguments rest on the premise that in the modern mass marketplace, consumer choice about privacy is illusory; others point to the insoluble information problems that consumers confront in assessing privacy tradeoffs; and still others reject a priori the notion that market resolution of privacy policy is appropriate.[89] On any of these views, the problem is not market failure, but rather a more systemic incompetence of markets.

---

87. *See* Victor P. Goldberg, *Institutional Change and the Quasi-Invisible Hand*, 17 J.L. & ECON. 461, 468 n.15, 484-91 (1974); Friedrich Kessler, *Contracts of Adhesion – Some Thoughts About Freedom of Contract*, 43 COLUM. L. REV. 629 (1943); Todd D. Rakoff, *Contracts of Adhesion: An Essay in Reconstruction*, 96 HARV. L. REV. 1173 (1984); W. David Slawson, *Standard Form Contracts and Democratic Control of Law-Making Power*, 84 HARV. L. REV. 529, 538-42 (1971); William T. Vukowich, *Lawyers and the Standard Form Contract System: A Model Rule That Should Have Been*, 6 GEO. J. LEGAL ETHICS 799, 800-11 (1993); *see also* Robert P. Merges, *Intellectual Property and the Costs of Commercial Exchange: A Review Essay*, 93 MICH. L. REV. 1570, 1611-13 (1995) (examining standard form terms within the narrower context of antitrust-style market power).

88. *See, e.g.*, Cohen, *Examined Lives*, *supra* note 2; Schwartz, *Privacy and Democracy*, *supra* note 71.

89. *See supra* Part III.A.2.

It is a measure of the degree to which both academic and policy debates have been captured by the rhetoric of markets and private ordering that arguments in this last group receive comparatively little attention. In the current climate, arguments from human dignity seem both insufficiently rigorous and vaguely passe. Yet the reluctance to address privacy in non-market terms is puzzling, for two reasons. As Jessica Litman has pointed out (and as privacy advocates "in the trenches" have always known), that is the way that ordinary people think about privacy.[90] Ordinary people—not academics, technologists, science fiction writers, or other members of the cyber-literati—react to abuses of privacy with outrage and a sense of betrayal, and feel that commercial dealings should be accompanied by privacy obligations.[91] That this outrage rarely translates into meaningful market resistance should not surprise us; if markets for privacy are inherently dysfunctional, there is no reason to expect this result.[92]

If one looks, instead, at other public policy-based limits on contract, the proposition that public policy should limit contractual waiver of privacy rights becomes much less remarkable than the rhetoric of current privacy debates makes it seem. Most people agree that there are some public policies that should not be altered by contract. Perhaps the best example is the general policy that one may not contract into a state of slavery, but there are many other, less dramatic examples. One is the rule that one may not sell one's organs for transplant, research, or any other use.[93] Two addi-

---

90. Jessica Litman, *Information Privacy/Information Property*, 52 STAN. L. REV. 1283, 1305-09 (2000).

91. *See id.*; LAURA J. GURAK, PERSUASION AND PRIVACY IN CYBERSPACE: THE ONLINE PROTESTS OVER LOTUS MARKETPLACE AND THE CLIPPER CHIP (1997).

92. The lack of market resistance by consumers is routinely invoked by privacy opponents as purportedly demonstrating a lack of genuine public concern with privacy. *See, e.g.*, Solveig Singleton, *Electronic Commerce: The Current Status of Privacy Protections for Online Consumers: Hearing Before the Subcomm. on Telecomm., Trade and Consumer Protection of the House Comm. on Commerce*, 106th Cong. (July 13, 1999), *available at* http://www.cato.org/testimony/ct-ss071399.html; Privacilla.org, *Comparing Privacy Polls and Consumer Behavior*, *at* http://www.privacilla.org/fundamentals/pollsand behavior.html (last visited Mar. 21, 2003) (pointing out that "[r]eal preferences are revealed by consumer's actions. . . ").

93. *See, e.g.*, 42 U.S.C. § 274e (2000); Newman v. Sathyavaglswaran, 287 F.3d 786, 794 (9th Cir. 2002); Perry v. Saint Francis Hosp. & Medical Ctr., 886 F. Supp. 1551, 1565 (D. Kan. 1995); Wilson v. Adkins, 941 S.W.2d 440 (Ark. Ct. App. 1997). This prohibition is grounded in a public policy against reducing the human body to a marketable commodity. Also void, under a similar rationale, are contracts for sexual services and contracts for the sale of children to adoptive parents. *See, e.g.*, Marvin v. Marvin, 557 P.2d 106, 109 (Cal. 1976) (sexual services); Downs v. Wortman, 185 S.E.2d 387 (Ga.

tional examples are the rules that providers of health care and of mass-marketed products, respectively, may not contract out of medical malpractice liability or liability for a defective product even if the patient or customer asserts willingness to risk injury in return for a lower price.[94] Still another, more recent example is set forth in a New York trial court's ruling enjoining a software developer from forbidding licensees to publish critical reviews of its products.[95] In each of these situations, the question whether the "free market" might equilibrate in a way that preserves the default rule is considered irrelevant.

This brief list illustrates two salient points about the sorts of public policies that are considered "important" enough to trump contract. First, these policies bolster noneconomic values that run the gamut from bodily integrity to freedom of expression to human dignity and self-determination. Privacy in general and intellectual privacy in particular fall comfortably within this spectrum. Second and equally important, the appeal to public policy is not simply an appeal to logic or political theory, but also to visceral notions of fairness and human dignity. For privacy concerns to trump contract, privacy advocates must establish not only that privacy values are similar in kind to other public values that society has sought to preserve, but also that they are similarly compelling. Once convinced of this, courts could quite easily develop rules limiting privacy waivers just as they have limited contractual waivers in other contexts.

At bottom, the argument for limiting waiver of intellectual privacy rights is straightforward, and builds upon the argument in Parts II and III.A, above, about why intellectual privacy is important and why the law should recognize harms to intellectual privacy in the first instance. Argu-

---

1971) (adoption); Willey v. Lawton, 132 N.E.2d 34 (Ill. Ct. App. 1956) (same); Baxter v. Wilburn, 190 A. 773 (Md. 1937) (same).

94. *See* Wheelock v. Sport Kites, Inc., 839 F. Supp. 730 (D. Haw. 1993) (holding that release agreement barring gross negligence claims against manufacturer and provider of paraglider was void as against public policy); Tunkl v. Regents of Univ. of Cal., 383 P.2d 441 (Cal. 1963) (holding that required agreement releasing hospital from malpractice liability was void as against public policy); Westlye v. Look Sports, Inc., 22 Cal. Rptr. 2d 781 (Cal. App. 1993) (holding that "as is" and assumption of risk clauses in ski equipment rental agreement did not bar recovery for skiing injuries caused by defective ski); Henningsen v. Bloomfield Motors, Inc., 161 A.2d 69 (N.J. 1960) (holding that agreement disclaiming implied warranty of merchantability was void as against public policy); Ash v. N.Y. Univ. Dental Ctr., 564 N.Y.S.2d 308 (App. Div. 1990) (holding that required agreement releasing hospital from malpractice liability was void as against public policy).

95. *See* Press Release, Office of New York State Attorney General, Judge Orders Software Developer to Remove and Stop Using Deceptive and Restrictive Clauses (Jan. 17, 2003), *at* http://www.oag.state.ny.us/press/2003/jan/jan17a_03.html.

ments about markets and market failures aside, intangible invasions of intellectual privacy are capable of causing great harm to individuals, and of substantially undermining shared, nonmonetizable values. Such invasions compromise rights of self-determination and undermine human dignity by eliminating the "breathing space" for intellectual development. A decision to promote these values in the law of "privacy" while simultaneously enabling easy evasion of accountability via "contract" would be nothing short of perverse. Taking these intangible harms seriously requires a more consistent approach.

IV. BUILDING INTELLECTUAL PRIVACY INTO CODE

Although legal sanctions for invasion of intellectual privacy are essential to guarantee respect for the intellectual privacy rights of information users, both judicial and regulatory sanctions are second-best strategies for ensuring effective protection for all users. A far more effective method of ensuring that information users actually enjoy the privacy to which they are entitled would entail building privacy into the design of DRM technologies in the first instance. In such a world, legal protection for intellectual privacy would serve as backdrop to more proactive, privacy-regarding conduct by (most) providers of information goods. Taking privacy into account at the outset requires a different approach to designing DRM technologies, and also requires a process for ensuring that, once designed, more privacy-protective DRM technologies are actually put in place.

A. Value-Sensitive Design for DRM

The notion of value-sensitive design is an outgrowth of the interdisciplinary study of science, technology, and society. Careful attention to the social embeddedness of technologies reminds us that technologies themselves are social artifacts; they constitute and are constituted by social values and interests.[96] This insight, in turn, suggests that careful attention to values and value choices at the design stage might produce important payoffs. In particular, as elaborated by Batya Friedman and her colleagues, one might envision an iterative research and design process that includes conceptual analysis of the values and value tradeoffs implicated by different designs, technical investigation of the range of design possibilities, and empirical study of user experiences with and responses to different designs.[97] Efforts to identify and catalog relevant "values" must, of course,

96. For helpful expositions of these themes, see BIJKER, *supra* note 22; MACKENZIE, *supra* note 22; WINNER, *supra* note 22.

97. *See* Batya Friedman, Daniel C. Howe & Edward Felten, *Informed Consent in the Mozilla Browser: Implementing Value-Sensitive Design*, *in* PROCEEDINGS OF THE 35TH

be conducted with an appropriate degree of humility. Making these efforts, however, seems infinitely preferable to the alternative.

In context of DRM technologies, the value-sensitive design approach would consider design for maximum control as only one potential direction that a DRM infrastructure could take.[98] Alternatively, one might imagine developing a design process devoted to exploring the full range of values, both private and public, implicated in DRM design, identifying the range of possible designs that might accommodate those values, and operationalizing DRM in a way that preserves an acceptable balance among competing public goods and private and user interests. Of particular relevance here, a value-sensitive design process for DRM technologies would seek, among other things, to create rights management infrastructures for information goods that respect and seek to preserve user privacy.[99] Such infrastructures would have three components, which map to the three types of DRM functionality discussed in Part II.B.

The first component of value-sensitive design for DRM would involve investigation and development of flexible restrictions that minimize or reduce direct constraints on intellectual consumption within private spaces. Conceptually, direct restrictions on user behavior implicate (at least) two opposing values.[100] One is the strong presumption in favor of intellectual privacy, in both its informational and spatial entailments. Under this presumption, an information provider has no legitimate interest in controlling or even knowing about certain types of uses of intellectual goods within

---

HAWAII INTERNATIONAL CONFERENCE ON SYSTEM SCIENCES (2002), *available at* http://dlib2.computer.org/conferen/hicss/1435/pdf/14350247.pdf (last visited Mar. 31, 2003); Batya Friedman, Peter H. Kahn, Jr. & Alan Borning, *Value Sensitive Design: Theory and Methods*, UW CSE TECHNICAL REPORT (Feb. 12, 2001), http://www.ischool.washington.edu/vsd/vsd-theory-methods-tr.pdf (last visited Mar. 31, 2003); Batya Friedman, *Value-Sensitive Design: A Research Agenda for Information Technology* (Aug. 23, 1999), *at* http://www.ischool.washington.edu/vsd/VSD_Research_Agenda.pdf (last visited Mar. 31, 2003); *see also* BATYA FRIEDMAN, ED., HUMAN VALUES AND THE DESIGN OF COMPUTER TECHNOLOGY (1997) (collecting essays and case studies that explore the intersections between human values and technical design).

98. *See supra* Part II.B.1; *see also* Stefan Bechtold, *The Present and Future of Digital Rights Management: A Roadmap of Emerging Legal Problems* (unpublished manuscript, on file with author) (arguing that DRM technologies can take many possible forms, and that demonizing "DRM" oversimplifies the policy problems that society must confront).

99. For an argument that DRM infrastructures also should be designed to preserve user privileges available under copyright law, see Burk & Cohen, *supra* note 64.

100. Obviously there are others, including policies favoring access to and reuse of information for reasons independent of privacy. The discussion in the text is intended to be illustrative, not comprehensive.

private spaces. The other is the generally held belief, grounded in both economic and noneconomic policy considerations, that information providers do have a legitimate interest in controlling widespread commercial copying, and that this interest may extend in some circumstances to controlling private copying in order to prevent it from reaching a certain critical mass. Technically, then, the challenge lies in developing technical systems that preserve both enough privacy for users and enough control for rights owners.

Although reconciling these competing values presents a significant design challenge, the idea that functionality restrictions might be designed to preserve (a degree of) flexibility for private access and copying, while simultaneously protecting information providers against large-scale commercial copying, is not novel. One example of such a technology is the serial copy management system mandated by the Audio Home Recording Act, which allows the production of perfect first-generation copies but causes significant quality degradation in subsequent generations.[101] Another example is the DMCA's requirement that analog videocassette recorders be designed to allow consumers to time-shift some kinds of television programming.[102] Elsewhere, Dan Burk and I have argued that flexible restrictions similar to these are necessary to preserve basic user privileges established under copyright law, such as fair use.[103] For the reasons discussed in Part II.B.1, flexible or "imperfect" restrictions on the functionality of digital copies also would operate to preserve user privacy. A careful, iterative methodology, incorporating participation by the full range of interested parties, could help designers negotiate the challenges entailed in implementing planned imperfection.

Value-sensitive design for DRM also would investigate methods of building in limits on monitoring and profiling of individual users. Because most businesses need to collect and retain some information about their customers to manage orders, payments, and deliveries, technological limits on data collection and use cannot fully substitute for other, human-implemented safeguards. Nonetheless, DRM systems may be designed either to minimize or to maximize data collection, retention, extraction and use. To preserve the intellectual privacy of information users, DRM design

---

101. 17 U.S.C. § 1002 (2000). For a brief description of the serial copy management system mandated by the statute, see Edward Samuels, *Why Can't I Make Copies from Copies of My CDs?*, *available at* http://www.gigalaw.com/articles/2001-all/samuels-2001-04-all.html (last visited Apr. 12, 2003).

102. 17 U.S.C. § 1201(k)(2).

103. *See* Burk & Cohen, *supra* note 64, at 54-70.

should incorporate minimization principles.[104] In the cases where real-time monitoring of user conduct is deemed to provide some significant non-privacy-related benefit,[105] designers should consider whether the desired benefit can be achieved without capturing the precise identity of the user, or without tying users to content.[106] If not, and if the implementation ultimately chosen must reflect a choice between the benefit and user privacy, that choice should be made explicitly, and should be documented so that later designers, regulators, and courts can understand the tradeoffs involved.

Finally, a value-sensitive design approach to DRM technologies would consider the desirability of implementing limitations on self-help. For example, after weighing the full spectrum of values implicated by automated, punitive enforcement actions, designers might conclude that digital content files should never be programmed to self-destruct, or to deny access entirely, upon detecting impermissible actions by users. Alternatively, they might conclude that denial of access should be permissible, but only in certain clearly defined and extreme circumstances.

These proposals are necessarily quite general. Whether they would operate to guarantee meaningful levels of privacy for information users would depend upon the specific details of their implementation. Nor are the specific suggestions offered here necessarily the only or the best ones;

---

104. Minimization of data collection and use is a keystone of internationally-agreed fair information practices. *See* OECD GUIDELINES, *supra* note 75, at 15; Joel R. Reidenberg, *Resolving Conflicting International Data Privacy Rules in Cyberspace*, 52 STAN. L. REV. 1315, 1325-29 (2000). Partial research agendas for the project of incorporating minimization principles into the design of DRM systems are set forth in Joan Feigenbaum et al. , *Privacy Engineering for Digital Rights Management Systems*, 2320 LECTURE NOTES IN COMPUTER SCI. 76 (2002), *available at* http://www.cs.yale.edu/homes/jf/FFSS.pdf (last visited May 5, 2003); Larry Korba & Steve Kenny, *Towards Meeting the Privacy Challenge: Adapting DRM*, *in* PROCEEDINGS OF THE 2002 ACM WORKSHOP ON DIGITAL RIGHTS MANAGEMENT (Nov. 2002), *available at* http://crypto.standford.edu/DRM2002/KorbaKennyDRM20021.pdf (last visited May 4, 2003); Deirdre Mulligan & Aaron Burstein, *Supporting Limits on Copyright Exclusivity in a Rights Expression Language Standard*, at 15-16 (Aug. 13, 2002), *at* http://www.law.berkeley.edu/cenpro/samuelson/projects/drm/20020906-OASIS-SLTPPC-EPIC.pdf (last visited May 4, 2003).

105. As one example of such a benefit, Feigenbaum et al. cite traffic and quality-of-service modeling. See Feigenbaum et al., *supra* note 104, at 13. A desire to generate and sell profiles of users' intellectual preferences, in contrast, is privacy-related (albeit inversely) and would not count.

106. *See, e.g.*, Feigenbaum et al., *supra* note 104, at 17-19; Latanya Sweeney, *Privacy and Confidentiality, in Particular, Computational Disclosure Control*, *at* http://privacy.cs.cmu.edu/people/sweeney/confidentiality.html (last visited Feb. 21, 2003) (describing research program to develop theoretical models and tools for de-identification and anonymization of information in electronic databases).

an expert in the relevant technological fields could undoubtedly think of others. The point is simply that a value-sensitive design methodology exposes "DRM" as a concept that is susceptible of a wide range of meanings. Understanding the DRM design process as (necessarily) value-driven, and undertaking a thorough analysis of all of the values implicated by technologies for automated management of rights in intellectual goods, are essential first steps toward ensuring that design priorities shift to accommodate a broader range of human and social priorities.

B. Implementing a Value-Sensitive Design Process

Identifying the possibility of value-sensitive design for DRM is only half the battle. For privacy-regarding DRM technologies to move from the pages of academic articles onto the drawing board and ultimately into the marketplace, those who participate in or underwrite real-world design processes need incentives to expand their frames of reference. Law has a role to play here as well, although it is a very different role from that discussed in Part III. Law's role in structuring DRM standard-setting processes is to ensure that the formulation of technical standards by market actors takes public values, including privacy values, into account.

If, as several advocacy organizations have urged, the law were to specify a "bill of rights" for users of information goods, this would constrain DRM development initiatives to focus on public values as well as private ones.[107] In particular, rights of intellectual privacy could be specified at a sufficiently high level of generality to avoid dictating the choice of technical standards, while still conveying important information about the substance of the protection to be afforded. Thus, following the model set forth above, rights of intellectual privacy would include: the right not to be subjected to (unreasonably) intrusive constraints on the use of intellectual goods within private spaces; rights against monitoring of intellectual consumption and profiling based on intellectual preferences; and, in at least some circumstances, the right not to be subjected to electronic self-help that would disable access to lawfully acquired information goods. Development of technical standards and processes to effectuate these rights would be the content industries' affair.

Vigilant defenders of market ordering will object that this proposal improperly injects government into a process—standards development—

---

107. *See, e.g.*, DigitalConsumer.Org, *at* http://www.digitalconsumer.org (last visited Apr. 16, 2003). I am using the term "law" very generally here to encompass both legislation and regulation. A digital consumer's bill of rights could come from Congress, but it could also come from the FTC pursuant to its mandate to regulate "unfair" practices in commerce. *See supra* Part III.A.2.

that is quintessentially of, by, and for the market. It takes but a moment's reflection to see that this objection is simply the first cousin once removed of the old argument for market ordering of privacy rights. If the first-order "market for privacy" cannot accurately reflect the variety of values placed on privacy,[108] it is difficult to imagine how a second-order market for privacy standards, derived by inference from the first-order market for privacy, could possibly do so. Even assuming that the first-order market for privacy actually worked, a hypothetical second-order market for privacy standards would entail a number of additional complications.

First, the relevant market is not simply the "market for privacy" or the "market for privacy standards," but also the market for DRM-protected content and DRM technologies capable of rendering the content. In the first instance, that market is not an end-user market at all, but rather a market that consists of intermediary licensors and distributors of digital content. Although users have repeatedly shown that they will reward entrepreneurs who provide them with freedom and flexibility to use, manipulate, copy, and redistribute digital content, the costs of providing that freedom have risen sharply in the wake of a string of highly-publicized contributory infringement lawsuits against MP3.com, Napster, Sonicblue, and other innovators.[109] Increasingly, therefore, the rational strategy is to license content subject to DRM restrictions dictated by content providers, regardless of whether the intermediary might otherwise prefer a different strategy.

Second, the market for DRM technologies is also the market for DRM standards. Many copyright owners lack the technical expertise to develop DRM standards themselves, and must commission or convince others to do it for them. This means that end users and intermediaries are not the only customers in the market for DRM technologies; in the case of DRM standards, which precede market availability of DRM-protected content both conceptually and chronologically, the copyright industries are the customers. As DRM standards penetrate more deeply into general purpose software and hardware, this dynamic becomes a bit more complicated; for example, developers of computer operating systems and microprocessors must satisfy many constituencies. Many technology companies, however,

---

108. *See supra* Part III.A.2.

109. *See* A&M Records, Inc. v. Napster, Inc., 284 F.3d 1091 (9th Cir. 2002); A&M Records, Inc. v. Napster, Inc., 239 F.3d 1004 (9th Cir. 2001); UMG Recordings, Inc. v. MP3.com, Inc., 92 F. Supp. 2d 349 (S.D.N.Y. 2000); *In re* Aimster Copyright Litig., 2002 Copy. L. Rep. (CCH) ¶ 28,500 (N.D. Ill. 2002); Jim Hu, *Sonicblue Seeks Bankruptcy Protection*, CNET NEWS.COM (Mar. 21, 2003), *at* http://news.com.com/2100-1047-993647.html.

also seek to avoid "technological mandates" handed down by the government, and appear to perceive voluntary DRM development efforts as the lesser of two evils.[110]

Third, assuming that the average end user could easily penetrate the relative opacity of most mass-market computing infrastructures and master the complex technical terminology of DRM, market processes are not well suited to enable end users to exert positive, as opposed to negative, influence on the design of technical standards. The market that end users encounter in the first instance is the market for DRM-protected content. In that market, one can refuse to buy or can switch from one provider to another, but there are no mechanisms to allow one to communicate as a prospective matter the precise level of functionality that one wants. And because DRM technologies are network technologies,[111] it will become increasingly difficult for dissenters to opt out. The more deeply embedded in software and hardware DRM functionality becomes, the harder it will be to avoid by purchasing noncompliant equipment. Particularly as more and more desired features and services are bundled with DRM restrictions, the costs of opting out may rapidly come to outweigh the benefits.

DRM standards processes offer an opportunity for more reflective participation in the debate over DRM but, at least as currently constituted, still are not good vehicles for the incorporation of public values into DRM design. To the average end user of information goods, standards processes are arcane and relatively inaccessible proceedings. Organizations representing end users and other noncommercial interests have begun to take an interest in DRM standard-setting.[112] At present, however, their participation in these processes is largely on the sufferance of the content and technology industries. Not all standards processes include end user representation, and even in those that do, there is no assurance that end user griev-

110. *See, e.g.*, Declan McCullagh, *Antipiracy Detente Announced*, CNET NEWS.COM (Jan. 14, 2003), *at* http://news.com.com/2100-1023-980633.html.

111. *See* Mark A. Lemley & David McGowan, *Legal Implications of Network Economic Effects*, 86 CAL. L. REV. 479 (1998).

112. *See, e.g.*, Elect. Privacy Info. Ctr., *Digital Rights Management and Privacy*, *at* http://www.epic.org/privacy/drm/default.html (last visited Apr. 1, 2003) (providing information on EPIC's submission to the OASIS Rights Language Technical Committee and its response to the Federal Communications Commission's (FCC) Notice of Proposed Rulemaking (NPRM) on broadcast flag standards); Mulligan & Burstein, *supra* note 104 (submission by the Samuelson Law, Technology, and Public Policy Clinic at the University of California, Berkeley, to the OASIS Rights Language Technical Committee); Public Knowledge, *Broadcast Flag Filings*, *at* http://www.publicknowledge.org/reading-room/documents/admin-filings/broadcast-flag/filings.php#PKfiling (last visited Apr. 1, 2003) (submissions by Public Knowledge/Consumer's Union in response to the FCC's broadcast flag NPRM).

ances, once aired, will prospectively shape the standards that are brought to market.[113]

All of this tends to suggest that to enable a genuinely inclusive, value-sensitive design process for DRM standards and technologies, some actor external to these markets must identify and maintain the centrality of the relevant public values. I do not wish to be interpreted as arguing that the law should mandate the content of technical standards for DRM technologies, or that government actors would be good at supervising such a process. Government can be rather good, though, at mandating non-technical standards. In the non-digital world, we call these non-technical standards simply "rights" and "duties," and have long recognized that (at a fairly high level of abstraction) rights and duties set the parameters for markets. In the digital world, where technical architectures acquire greater regulatory force, an effective formulation of legal rights and duties must state (among other things) the values that technical standards should be designed to enable—or simply preserve.[114]

V. CONCLUSION

DRM technologies may represent the future of information access and use, but their design and implementation are still open questions. A shift to an information environment characterized by pervasive constraints, universal monitoring, and automated self-help would severely undermine in-

113. The DRM standards project sponsored by the Organization for the Advancement of Structured Information Standards (OASIS) emphasizes open, non-proprietary standards and is open to all interested parties. *See* OASIS, *Rights Language TC*, *at* http://www.oasis-open.org/committees/tc_home.php?wg_abbrev=rights (last visited Apr. 1, 2003). Other standards projects, including the copyright industry-driven Copy Protection Technical Working Group, *at* http://www.cptwg.org (last visited Apr. 1, 2003), and the Trusted Computing Platform Alliance initiated by Microsoft, Intel, IBM, Hewlett Packard, and Compaq, *at* http://www.trustedcomputing.org/tcpaasp4/index.asp (last visited Apr. 1, 2003), appear to have open membership policies, but only for corporate members. Many other DRM standards projects utilize neither open standards nor open membership. These include the motion picture industry's DVD Content Control Association, Microsoft's Next Generation Secure Content Base project, Intel's LaGrande project, and a host of smaller private efforts to develop proprietary DRM technologies. *See* Chris Gaither, *Intel Chip to Include Antipiracy Features, Some Still Fear Privacy of Users Will Be Violated*, BOSTON GLOBE, Sept. 10, 2002, at C3; Robert Lemos, *What's in a Name? Not Palladium*, CNET NEWS.COM (Jan. 24, 2003), *at* http://news.com.com/2100-1001-982127.html?tag=fd_top; *DVD Copy Control Association*, *at* http:/www.dvdcca.org (last visited Apr. 1, 2003).

114. *Cf.* LESSIG, *supra* note 17 (arguing that constitutional doctrine must be sensitive to the ways in which code regulates behavior); Reidenberg, *supra* note 17 (arguing that law- and policymakers should understand and exploit the regulatory functions of code).

tellectual privacy values. Instead, in the era of DRM, law and technology together must share responsibility for protecting intellectual privacy. Law can fulfill its responsibility in its usual fashion, by defining individual rights and correlative obligations, but to do so effectively it must come to terms with both the inadequacy of "markets for privacy" and the central role played by DRM standards in defining rights and obligations as a practical matter. Technology can fulfill its responsibility to the extent that its designers and their customers in the content industries practice both inclusiveness and restraint, but to do so effectively they must come to terms with the importance of law, and more broadly of public policy and public values, in establishing design parameters. The time to undertake these tasks is now, before highly restrictive technical proposals and highly permissive legal responses harden into legacies that may prove far more difficult to dislodge.

WILL MERGING ACCESS CONTROLS AND RIGHTS CONTROLS UNDERMINE THE STRUCTURE OF ANTICIRCUMVENTION LAW?

By R. Anthony Reese[†]

ABSTRACT

Copyright owners are increasingly using technological measures, often referred to as "digital rights management" systems, to protect their works in digital formats. In 1998, Congress granted copyright owners legal remedies against the circumvention of such measures and against the suppliers of circumvention technologies. This Article considers how the complex structure of these legal protections might affect copyright owners' choices of which technological measures to deploy. Because Congress provided stronger protection to measures controlling access to copyrighted works than it provided to measures controlling copyright owners' rights in those works, copyright owners might prefer access controls to rights controls. In practice, however, copyright owners may be able to employ technological protection systems that incorporate both an access control and a rights control. So far, courts have treated such "merged" control measures as entitled to the legal protections afforded *both* access-control and rights-control measures. The Article next considers the impact on consumers of copyright owners' use of merged control measures. Congress expressly provided less protection for rights controls in order to allow consumers to make noninfringing uses of copyrighted works in protected digital format. By protecting merged control measures as both access controls and rights controls, courts may undermine this congressional scheme for balancing protections for copyright owners and the public's interest in noninfringing use. Finally, the Article explores possible responses to the potential threat posed by the deployment of merged control measures, including amending the legal protections for technological control measures to allow the circumven-

---

† Assistant Professor, School of Law, The University of Texas at Austin. B.A., Yale University; J.D., Stanford Law School. I thank Graeme Dinwoodie, Paul Goldstein, and Christopher Leslie for comments on earlier drafts. I thank Beth Youngdale of the Tarlton Law Library for research assistance.

tion of a merged control measure where the post-circumvention use of the protected work is noninfringing.

TABLE OF CONTENTS

I. INTRODUCTION

Copyright owners show increasing interest in using technological measures, often referred to as "digital rights management" (DRM) systems, to protect their works in digital formats and control access to and use of those works. In 1998, Congress added a new chapter to U.S. copyright law, Chapter 12 of Title 17,[1] providing copyright owners who use such technological control measures with legal remedies against the circumvention of those measures and against the suppliers of devices or technologies that accomplish such circumvention.

This Article considers how these new legal protections potentially impact copyright owners' choices about the type of technological control measures to employ with their works. The type of control measures copyright owners choose will, of course, depend on a variety of factors in addition to the legal protections, including availability, effectiveness, cost, and

1. 17 U.S.C. §§ 1201-1205 (2000).

consumer acceptance.[2] But at least in part, the nature and degree of legal protection available against circumvention will likely influence the choice of which control measures to adopt.

Part II looks at how the complex structure of legal protections in Chapter 12 might affect copyright owners' choices. In particular, this Part examines the different legal protection afforded to the two types of technological control measures protected by the statute: access-control measures and rights-control measures. Because access controls may enjoy stronger protection under the statute than rights controls, copyright owners may prefer access controls to rights controls.

In practice, however, copyright owners may not need to choose between the different types of legal protections available. Copyright owners may instead be able to employ technological protection systems that incorporate both an access control and a rights control. So far, courts have treated such "merged" control measures as entitled to the legal protections of *both* access- and rights-control measures, even when the system was essentially directed only at preventing copying and distribution, rather than at controlling access. If courts continue to treat merged control measures in this manner, copyright owners may have an incentive to use such merged controls in order to maximize their legal protection.

Part III considers the impact on consumers of copyright owners' use of merged control measures and the courts' strong protection of such control measures. Congress expressly provided less protection for rights controls in order to allow consumers to make noninfringing uses of copyrighted works in protected digital format, just as consumers have for centuries made noninfringing uses of copyrighted works in unprotected analog copies. By protecting merged control measures as both access controls and rights controls, courts may undermine this congressional purpose by preventing consumers from legally engaging in conduct with respect to merged control measures that would be legal with respect to rights-control measures.

The deployment of merged control measures thus poses a threat to the congressional scheme for balancing protections for copyright owners against the public's interest in noninfringing use. Part IV explores possible responses to this threat. One response is to amend Chapter 12's legal pro-

---

2. *See, e.g.*, Pamela Samuelson, *Intellectual Property and the Digital Economy: Why the Anti-Circumvention Regulations Need to Be Revised*, 14 BERKELEY TECH. L.J. 519, 566 (1999) ("Competition among information providers may also affect the successful deployment of technical protection systems. If one information provider tightly locks up his content, a competing provider may see a business opportunity in supplying a less tightly restricted copy to customers who might otherwise buy from the first provider.").

tections to allow the circumvention of a merged control measure where the circumventing party's post-circumvention use of the protected work is noninfringing. This Part further explores some of the implications of such a proposal. While exempting such circumvention might be possible by means of a rulemaking procedure provided for in the statute, congressional action is probably necessary.

II. LIKELY PRACTICAL IMPACT ON COPYRIGHT OWNERS OF THE DIFFERENT LEGAL PROTECTION FOR ACCESS CONTROLS AND RIGHTS CONTROLS

A. Contrasting Access Controls with Rights Controls

The anticircumvention provisions of Chapter 12 carefully distinguish between two types of technological protection measures: any measure that "effectively controls access to" a copyrighted work;[3] and any measure that "effectively protects a right of a copyright owner" under U.S. copyright law.[4] The scope of legal protection given to each type of technological control varies.[5]

1. Access Controls Receive Greater Statutory Protection

Both access-control and rights-control measures are protected against the manufacture and distribution of devices and technologies that circumvent the measures.[6] The statute essentially makes no distinction between devices that circumvent access- or rights-control measures with respect to outlawing such circumvention technologies and devices.[7] Thus, if a product or service is primarily designed or produced to circumvent an access control or a rights control, or has only limited commercially significant

3. 17 U.S.C. § 1201(a)(1)(A), (a)(2).

4. *Id.* § 1201(b)(1).

5. In the European Union, by contrast, "the same protection is granted to technologies controlling access and to technologies protecting rights (e.g. copy control technology)." Maria Martin-Prat, *The Relationship Between Protection and Exceptions in the EU "Information Society" Directive*, *in* ADJUNCTS AND ALTERNATIVES TO COPYRIGHT 466 (Jane C. Ginsburg & June M. Besek eds., 2002).

6. The language of the bans is quite broad. The bans provide that no one shall "manufacture, import, offer to the public, provide, or otherwise traffic in any technology, product, service, device, component, or part thereof" that meets certain criteria. 17 U.S.C. § 1201(a)(2), (b).

7. Actually, while the basic prohibitions on manufacture of and trafficking in circumvention technologies make no distinction based on the type of control measure being circumvented, certain of the exceptions to those basic prohibitions on devices do distinguish between access controls and rights controls. *See infra* text accompanying notes 66-67.

purpose or use other than to circumvent such a control, or is knowingly marketed for use in circumventing such a control, then the manufacture or distribution of the product or service is illegal.[8]

The distinction between access controls and rights controls becomes significant, though, for the second type of legal protection that Chapter 12 offers to technological protection measures. The statute in some cases bars the very act of circumventing a technological control. However, the ban applies only to acts of circumventing *access* controls[9] and not *rights* controls. A person who circumvents an access-control measure violates § 1201(a)(1)(A) and is subject to the civil remedies of § 1203 (including statutory damages of up to $2,500 per act).[10] If the circumvention is done "willfully and for purposes of commercial advantage or private financial gain," the circumventor is subject to the criminal provisions of § 1204 (including a fine of up to $500,000 and up to five years in prison for a first offense).[11]

On the other hand, a person who circumvents a rights-control measure does not commit any violation of § 1201, and is not subject to any remedies or penalties under § 1203 and § 1204.[12] Instead, such a circumventor is subject only to liability for copyright infringement under § 501(a).[13] Such liability turns not on the fact that the person circumvented the rights control, but rather on ordinary principles of copyright law as applied to the actions the circumventor took after the circumvention. Did she engage in an act of reproduction, distribution, adaptation, or public performance or display reserved exclusively to the copyright owner under § 106? Was her act authorized by the copyright owner, either expressly or impliedly, or was it excused by one of the specific limitations on the copyright owner's rights contained in §§ 107 through 122 of the Copyright Act? The Senate Report on the DMCA, in explaining the absence of a ban on acts that circumvent rights-control measures, makes this clear:

---

8. 17 U.S.C. § 1201(a)(2), (b)(1).

9. *See id.* § 1201(a)(1)(A).

10. *Id.* § 1203(c) (establishing civil remedies for any injury caused "by a violation of section 1201 or 1202"). A plaintiff alleging a § 1201 violation can pursue either actual or statutory damages. *See id*.

11. *Id*. § 1204(a) (imposing criminal penalties for such violations of § 1201 or § 1202).

12. "Section 1201(b) . . . does not prohibit direct acts of circumvention; the technologically adept user thus faces no liability under that section." Jane C. Ginsburg, *Copyright Legislation for the "Digital Millennium"*, 23 COLUM.-VLA J.L. & ARTS 137, 143 (1999).

13. *See* 17 U.S.C. § 501(a).

> It is anticipated that most acts of circumventing a technological copyright protection measure will occur in the course of conduct which itself implicates the copyright owners[’] rights under title 17. This subsection is not intended in any way to enlarge or diminish those rights. Thus, for example, where a copy control technology is employed to prevent unauthorized reproduction of a work, the circumvention of that technology would not itself be actionable under 1201, but any reproduction of the work that is thereby facilitated would remain subject to the protections embodied in title 17.[14]

In many instances, of course, one who circumvents a rights control will not infringe the copyright owner’s rights in violation of “the protections embodied in title 17.” She may reproduce part of the work, but her reproduction may qualify as fair use or as consumer noncommercial making of a musical recording, both of which are not infringements.[15] She may publicly display the work, but that display might be authorized because it is made to an audience located at the same place as the lawfully made copy of the work from which the display was made.[16] She may publicly perform the work in the course of face-to-face teaching activities in a classroom of a nonprofit educational institution, as allowed by copyright law.[17] The wrongfulness of the circumventor’s actions thus turns not on her act of circumventing a technological measure that protects a copyright owner’s exclusive rights, but rather on whether her actions infringe upon those exclusive rights, as limited by statutory provisions and common law doctrines.

The additional protection offered against acts of circumventing access controls but not rights controls offers some incremental protection to copyright owners. Since acts circumventing access-control measures will often take place in private, they will be no more likely to be detected (or to result in enforcement efforts) than individuals’ private acts of reproduction (such as home taping, CD burning, or photocopying) have been under

---

14. S. REP. NO. 105-190, at 29 (1998).

15. *See* 17 U.S.C. § 107 (providing that fair use of copyrighted material does not constitute infringement); *id*. § 1008 (providing that no action may be brought under Title 17 based on noncommercial use by a consumer of an audio recording device to make musical recordings).

16. *See id*. § 109(c). For an in-depth discussion of noninfringing public displays, see R. Anthony Reese, *The Public Display Right: The Copyright Act’s Neglected Solution to the Controversy Over RAM “Copies”*, 2001 U. ILL. L. REV. 83, 86-92.

17. *See* 17 U.S.C. § 110(1).

modern copyright law.[18] An individual who circumvents an access-control measure in order to watch in private her own copy of a film that is region-coded or time-limited in order to prevent its performance seems no more likely to be sued by a copyright owner for violating § 1201(a)(1)(A) than an individual who records a television broadcast of a motion picture in order to repeatedly view it later is likely to be sued for copyright infringement.[19]

In some cases, however, someone who circumvents an access control will go beyond a mere private act of circumvention and will engage in more detectable activities which could lead to enforcement of the circumvention ban. The circumventor might make copies of the work and distribute them to the public, or might transmit performances or displays of the work over computer networks using, for example, peer-to-peer software. In those instances, a copyright owner might well detect the circumventing party's public, post-circumvention uses of the work. For example, someone who acquires a digital copy of a film protected by an access control that allows viewing the film for any single twenty-four-hour period, and who then circumvents the access control after the twenty-four hour period in order to copy the film, is more likely to be detected if she posts the copy she made on a peer-to-peer network than if she simply views it in her own home. The circumventing party in such circumstances is, of course, liable for any infringements of the copyright owner's exclusive rights under § 106. In the course of investigating or litigating the infringement claim, however, the copyright owner might also uncover the pre-infringement

18. *See, e.g.*, Glynn S. Lunney, Jr., *The Death of Copyright: Digital Technology, Private Copying, and the Digital Millennium Copyright Act*, 87 VA. L. REV. 813, 830 (2001) (noting that because "enforcing the [act] prohibition will require lawsuits against each individual user" of circumvention technology, the "prohibition will prove largely impractical to control widespread private copying"); Neil Weinstock Netanel, *Impose a Noncommercial Use Levy to Allow Free P2P File Sharing*, 17 HARV. J.L. & TECH. (forthcoming 2003) ("Merely fortifying DRM controls with a prohibition against individuals' circumvention would have left copyright holders facing much the same enforcement costs and public relations risks as suing individual infringers under traditional copyright law."); Samuelson, *supra* note 2, at 554-55 (noting that the initial executive branch proposal on circumvention contained no bar on any acts of circumvention and suggesting that the drafters may have believed that "it would be difficult to detect individual acts of circumvention, and as long as such acts were done on an isolated, individual basis (due to the unavailability of circumvention devices), the danger to copyright owners would be small").

19. Such recording would not qualify as fair-use "time shifting" allowed by *Sony*, since the practice approved there involved taping broadcast material in order to watch it at another time and then erasing it. *See* Sony Corp. v. Universal City Studios, Inc., 464 U.S. 417, 423 (1984).

circumvention of the access-control measure. That would permit the copyright owner to pursue an additional cause of action against the circumventor for violation of § 1201. The copyright owner would presumably be entitled to relief for the act of circumvention, particularly statutory damages and possible treble damages, in addition to the relief available for the copyright infringement. Thus, while copyright owners may not need the ban on acts of circumvention in order to have some legal recourse against those who both commit such acts *and* are likely to be detected doing so,[20] that ban does give copyright owners additional relief against such parties.[21]

In other instances, a party circumventing an access-control measure may face liability for her circumvention even though she is not liable for copyright infringement for her post-circumvention activities. For example, a person who circumvents a measure controlling access to a copyrighted work in order to engage in a fair use, such as creating a parody of the copyrighted work, and who then publicizes the parody, would not be liable under copyright law for making the parody available to the public. However, she may face liability under § 1201 because by making the parody publicly available she has revealed her act of circumvention.[22] In this case, the copyright owner would not have a viable infringement claim against the circumventing party, since the circumventor's use of the copyrighted work qualifies as a fair use. However, having revealed (at least indirectly) her act of circumvention, the parodist is subject to suit for circumventing

20. In addition, there is no need to impose liability on acts of circumvention in order to impose secondary liability on those who contribute to acts of circumvention by providing equipment or technology to do so, since § 1201(a)(2) and § 1201(b) directly impose liability on those who supply such equipment. In the context of copyright infringement, on the other hand, prohibiting private and likely undetectable acts of reproduction, performance, or display may be necessary for the imposition of liability for contributory infringement on those who facilitate such private activities, given the general view that some act of direct copyright infringement must occur in order for one to be held liable for contributory infringement. *See id.* at 434-42; 2 PAUL GOLDSTEIN, COPYRIGHT § 6.3.2, at 6:44 (2d ed. 1996 & 2000 Supp.) ("Courts, including the United States Supreme Court, have universally held that, for a defendant to be contributorily or vicariously liable, a direct copyright infringement must have occurred.").

21. *See* Thomas Vinje, *Copyright Imperilled?*, 1999 EUR. INTELL. PROP. REV. 192, 198 ("Where damages are awarded or penalties imposed for circumvention in addition to those available for copyright infringement, the addition of a prohibition on circumvention could provide a significant supplemental deterrent to copyright infringement.").

22. While the public dissemination of the parody would not necessarily provide direct evidence of the circumvention, if the copyrighted work had been distributed only in protected formats, then the dissemination of the transformed copy of the work might offer circumstantial evidence of the act of circumvention, and discovery during litigation might confirm that such circumvention took place.

the access control to engage in her noninfringing, transformative copying and potentially liable at least for statutory damages of up to $2,500 per circumventing act.[23] Thus, in such instances, the ban on circumventing access-control measures offers a copyright owner legal recourse against a user where copyright law itself might give no relief.

In sum, Chapter 12 "gives the greatest protection to copyright owners' right to control access" because it "tolerates direct end-user circumvention of post-access anticopying measures, to a far greater extent than it does circumvention of access controls."[24] The greater protection for access controls may have practical benefits for copyright owners adopting DRM measures. Where an act of circumvention is detectable, Chapter 12 offers copyright owners relief against circumventors that goes beyond any relief available for the copyright infringement and offers the only potential relief against circumventing parties whose post-circumvention activities do not amount to copyright infringement. Such relief is unavailable against those who circumvent rights controls, and therefore access controls are likely to prove more attractive to copyright owners.

2. Courts May Interpret the Statute to Give Access Controls Greater Legal Protection Against Circumvention Devices

Access controls receive greater protection under Chapter 12 than do rights controls, since only access controls are protected against acts of circumvention. But even with respect to the ban on disseminating circumvention technologies, which applies to both types of control measures, Chapter 12 may, depending on how courts interpret its language, offer stronger or more certain protection to access-control measures than to rights-control measures.

Any measure that effectively controls "access" to a work is protected under Chapter 12. The term "access" is never defined,[25] but is likely to be read broadly, probably extending to any act by which the work is made

---

23. 17 U.S.C. § 1203(c)(3) (2000). Alternatively, the copyright owner could pursue her actual damages and any profits earned by the violator. *Id.* In addition, the circumventor could face the impoundment and destruction of any computer equipment used in her circumvention. *See id.* § 1203(b)(2), (6).

24. Ginsburg, *supra* note 12, at 139.

25. The statute does define when a technological measure "effectively controls access to a work" as "if the measure, in the ordinary course of its operation, requires the application of information, or a process or a treatment, with the authority of the copyright owner, to gain access to the work." 17 U.S.C. § 1201(a)(3)(B). This definition in no way narrows the concept of "access" protected by § 1201.

perceptible.[26] Thus, any measure that controls a user's ability to perceive a work will likely qualify for protection under § 1201(a), and technologies circumventing any such control will be outlawed unless they have some other commercially significant purpose.

Technological control measures may have more difficulty qualifying for protection as rights-control measures, partly because a copyright owner's rights are constrained by exceptions. A rights-control measure is one that effectively protects a right of a copyright owner under the Copyright Act. Although the copyright owner's rights are quite broad, encompassing reproduction, distribution, adaptation, public performance, and public display,[27] they are nevertheless subject to numerous limitations and exemptions. First, the copyright owner's rights extend only to public performances and displays; all private performances and displays are entirely outside the scope of the copyright owner's rights.[28] So someone who plays recorded music on CD or a film on DVD in the privacy of her own home is in no way exercising any right of the copyright owner. Second, the statutory grant of exclusive rights to copyright owners is subject to express exceptions.[29] Certain acts are outside the scope of the copyright owner's exclusive rights and are therefore not infringing, even though they are acts of reproduction, distribution, adaptation, public performance, or public display. For example, it is not copyright infringement for teachers or students of a nonprofit educational institution to perform a copyrighted work in a classroom in the course of face-to-face teaching activities,[30] even though the teacher or students would be performing the work "publicly" as

---

26. *See* Jane C. Ginsburg, *From Having Copies to Experiencing Works: The Development of an Access Right in U.S. Copyright Law*, *in* U.S. INTELLECTUAL PROPERTY 2 (Hugh Hansen ed., 2000), *available at* http://papers.ssrn.com/sol3/papers.cfm?abstract_id=222493 ("Every act of perception or of materialization of a digital copy requires a prior act of access."); *id.* at 12 ("Thus, 'access to the work' becomes a repeated operation; each act of hearing the song or reading the document becomes an act of 'access.'"); GOLDSTEIN, *supra* note 20, § 5.17.1, at 5:245 ("Access to a work in the sense evidently contemplated by section 1201(a) occurs any time a user derives value from a work without necessarily infringing one of the exclusive rights secured by copyright.").

27. 17 U.S.C. § 106.

28. Indeed, not every work enjoys exclusive performance and/or display rights. Most significantly, sound recording copyright owners have no general exclusive right to perform or display their works publicly. *Id.* §§ 106(4), 114(a). They do, however, have a narrow right to perform their works publicly by means of a digital audio transmission. *Id.* § 106(6).

29. 17 U.S.C. § 106 grants exclusive rights to copyright owners and is subject to exceptions provided in §§ 107-122.

30. *Id.* § 110(1).

the Copyright Act defines that term.[31] As a result of the express exceptions, the rights of the copyright owner are not the very broadly stated exclusive rights of reproduction, adaptation, distribution, public performance, and public display. Instead, the copyright owner has the rights to reproduce, distribute, adapt, and publicly perform or display her work "exclusively" only to the extent that the statute does not expressly permit such activities by other people.

Technological protection measures that control reproduction or performance of a work, however, are unlikely to be well calibrated to the actual contours of, for example, copyright owners' reproduction or public performance rights.[32] Consider a technological control measure on the performance of a motion picture in a format such as a DVD. Perhaps the control measure requires the user of the DVD to enter a code before the film can be performed, possibly a code unique to the DVD player on which the disc was first played, thus essentially "tethering" the particular disc to a particular player.[33] The control measure would most likely require entry of the code for *any* performance of the film, whether it is to be viewed by an individual in a private residence (a private performance entirely outside the scope of the § 106(4) right), by a class of students (a public performance, but one permitted under § 110(1)), or by an admission-paying audience in an auditorium (a public performance within the copyright owner's exclusive rights). In the case of the auditorium showing, the control measure effectively protects the copyright owner's rights by limiting the exercise of the public performance right under § 106(4). In the other two cases, however, the control measure does not limit the exercise of the copyright owner's public performance right. Instead, the measure controls the user's ability to engage in performances that are entirely noninfringing and out-

31. *See id*. § 101 ("publicly"). That definition includes performing a work "at any place where a substantial number of persons outside of a normal circle of a family and its social acquaintances is gathered," which would probably be the case in many classroom settings. *Id*.

32. *See* Dan L. Burk & Julie E. Cohen, *Fair Use Infrastructure for Rights Management Systems*, 15 HARV. J.L. & TECH. 41, 55-57 (2001) ("At least for now, there is no feasible way to build rights management code that approximates both the individual results of judicial determinations and the overall dynamism of fair use jurisprudence."); Julie E. Cohen, *Some Reflections on Copyright Management Systems and Laws Designed to Protect Them*, 12 BERKELEY TECH. L.J. 161, 177 (1997) ("Automated [copyright management systems] are inherently ill-equipped to handle the equitable, fact-specific inquiry required in fair use cases.").

33. For a discussion of "tethered" copies, see R. Anthony Reese, *The First Sale Doctrine in the Era of Digital Networks*, 44 B.C.L. REV. (forthcoming May 2003); U.S. COPYRIGHT OFFICE, DMCA SECTION 104 REPORT 75 (2001), *available at* http://www.copyright.gov/reports/studies/dmca/dmca_study.html.

side the scope of the copyright owner's exclusive rights.[34] Is such a measure protected under § 1201(b)? Is it illegal to manufacture and distribute a device that circumvents such a control measure?

Section 1201(b) protects a technological control measure if the control "effectively protects a right of a copyright owner under [Title 17]," which means that "the measure, in the ordinary course of its operation, prevents, restricts, or otherwise limits the exercise of a right of a copyright owner under this title."[35] The tethering control effectively protects the copyright owner's public performance right—at least in cases where the user of the DVD performs the work publicly. After all, some of the activity controlled by the measure—e.g., showing the film to paying viewers in an auditorium—is within the copyright owner's rights. The difficulty, however, is that much of the activity controlled by the measure is *not* within those rights. But because the statute does not say that a control measure must *only* control against infringing activities, the tethering control may qualify as a control measure that effectively protects a right of the copyright owner.

It is not clear, though, that a device circumventing such a broadly targeted control measure would be prohibited under § 1201(b). That section essentially outlaws circumvention technology if it is "primarily designed or produced for the purpose of," or if it "has only limited commercially significant purpose or use other than," circumventing the protection afforded by a rights-control measure.[36] What of a technology that enables a user to circumvent a copyright owner's control measure where that measure prevents the user not from engaging in activity reserved to the copyright owner but in an entirely noninfringing activity, such as privately performing a motion picture? What of a device that allows a person to take a DVD "tethered" to her home DVD player and play it on a different DVD player in a friend's home? Arguably, that device has the use of circumventing a technological measure that interferes with lawful activity—privately performing a copyrighted motion picture—rather than (or in addition to) circumventing a technological measure that protects a right of the copyright owner. If that use is of more than limited commercial sig-

34. A measure preventing the copying of recorded music is another example of a measure that would limit a user's ability to engage both in conduct reserved to the copyright owner *and* conduct permitted to the user under Title 17. Section 106(1) gives copyright owners the exclusive right to reproduce musical works and sound recordings, but § 1008 allows a consumer to make "noncommercial" copies of recorded music. *See* 17 U.S.C. §§ 106(1), 1008.

35. *Id*. § 1201(b)(2)(B).

36. *Id*. § 1201(b)(1)(A)-(B).

nificance, then the device might not be barred by § 1201(b)(1), which only outlaws devices that circumvent rights controls.[37]

The statute might nevertheless be read to ban such a device. Section 1201(b)(1) outlaws technologies that circumvent "protection afforded by a technological measure that effectively protects a right of a copyright owner."[38] Thus, for example, circumventing a tethering control in order to privately perform a copyrighted work might be considered circumventing "protection afforded by" a rights-control measure, even though that measure's protection is not, in that instance, directed to a right of a copyright owner. Under this broad reading of the statute, as long as a control measure in *any* way protects a copyright owner's rights *in addition to* controlling legitimate, noninfringing activities, then a technology's ability to circumvent the measure in order to allow such legitimate, noninfringing activities would be irrelevant to determining whether the circumvention technology is lawful.

This broad reading might find support in the different language Congress used in the access-control and rights-control device bans. In § 1201(a), Congress banned devices that "circumvent a technological measure" that controls access to a work, while in § 1201(b), Congress banned devices that "circumvent *protection afforded by* a technological measure" that protects a right in a work.[39] This difference in terminology could reflect a congressional intention to provide broader protection in § 1201(b). Read this way, § 1201(b) would outlaw devices that circumvent any protection provided by a rights-control measure, even if the protection in that instance was not itself directed at activity within the scope of the copyright owner's rights.

At least one court has treated § 1201(b) in this broad manner with respect to devices that could be used to circumvent a rights-control measure in order to engage in fair use of a protected work. *United States v. Elcom Ltd.*[40] involved a computer program that circumvented technological measures used by e-book reader software to prevent copying, printing, lending, and reading aloud of e-books.[41] The court acknowledged that the defendant's software enabled the lawful owner of an e-book to engage in

37. Because the bans in § 1201(b)(1) are cumulative, in order to be legal, the device must also not have been primarily designed or produced for circumvention nor be marketed for circumvention.

38. 17 U.S.C. § 1201(b)(1)(A)-(C).

39. *Id.* § 1201(b) (emphasis added). *Compare, e.g.*, *id.* § 1201(a)(2)(A) *with id.* § 1201(b)(1)(A).

40. 203 F. Supp. 2d 1111 (N.D. Cal. 2002).

41. *See id*. at 1118.

noninfringing conduct, such as reading the e-book on a different computer than the one onto which it was originally downloaded or making a backup copy of the book.[42] The court further acknowledged the problem with § 1201(b)'s definition of rights-control measures arising out of the fact that "the rights of a copyright owner are intertwined with the rights of others" because of the statutory exceptions to the copyright owner's exclusive rights.[43] The court nonetheless held that all devices that circumvent rights control measures are prohibited by the statute, even if the circumvention is made in order to enable a fair use outside the scope of the copyright owner's rights. The court stated that "all tools that enable circumvention of [rights controls] are banned, not merely those [rights controls] that prohibit infringement."[44]

Reading § 1201(b)'s device ban so broadly poses a number of interpretive difficulties, though. As to the apparently broader language of § 1201(b)'s device ban as compared to § 1201(a)'s ban, Congress actually defined the phrase "circumvent protection afforded by a technological measure" to mean "avoiding, bypassing, removing, deactivating, or otherwise impairing *a technological measure*,"[45] suggesting that Congress did not perceive any difference between circumventing a technological measure and circumventing the protection afforded by a technological measure. And at the point in the legislative history when the distinction in phrasing and definition between § 1201(a) and § 1201(b) appeared,[46] no one seems

---

42. *See id*. at 1118-19.

43. *Id.* at 1121.

44. *Id.* at 1124.

45. 17 U.S.C. § 1201(b)(2)(A).

46. The language of the device bans in § 1201(a)(2) and § 1201(b)(1), and the associated definitions, are virtually unchanged from the language in companion bills H.R. 2281, 105th Cong. (1997) and S. 1121, 105th Cong. (1997), the first bills introduced to implement the WIPO Copyright Treaty anticircumvention requirements. In the 104th Congress, the NII Copyright Protection Act of 1995, H.R. 2241, 104th Cong. (1995) and S. 1284, 104th Cong. (1995) contained the first proposed version of § 1201, but that one-paragraph version made no distinction between access controls and rights controls, did not outlaw any acts of circumvention, and did not include the language and definitions under discussion. Nevertheless, the drafters of the anticircumvention provisions of the NII Copyright Protection Act expressly indicated that circumvention devices that enabled noninfringing uses would not necessarily be prohibited:

> The Working Group recognizes . . . that . . . certain uses of copyrighted works are not unlawful under the Copyright Act. Therefore, the proposed legislation prohibits only those devices or products, the primary purpose or effect of which is to circumvent such [technological protection] systems *without authority*. That authority may be granted by the copyright owner *or by limitations on the copyright owner's rights under the Copyright Act.*

to have expressly indicated that the distinction was designed to outlaw circumvention devices that allowed users to engage in legitimate, noninfringing activities.

Indeed, Congress may have used two different phrases simply to avoid confusion between the definitions of "circumvent" in the two subsections. Each phrase is expressly defined in its own subsection. The definition of "circumvent a technological measure" in § 1201(a) is more detailed, giving the examples of descrambling a scrambled work and decrypting an encrypted work, in addition to the more general list of avoiding, bypassing, removing, deactivating, or impairing a technological measure.[47] In contrast, the definition of "circumvent protection afforded by a technological measure" in § 1201(b) only provides the general list and not the specific examples.[48]

Perhaps the most significant interpretive difficulty with reading § 1201(b) so broadly is that such a reading renders the statute's elaborate distinction between rights controls and access controls largely, if not entirely, superfluous. Under such a reading of the section, every access control would automatically be a rights control as well.

Access to a work stored in digital format requires the ability to perceive that work: to see the text, hear the recorded sound, and view the visual images. In the analog world, human beings in many cases can directly perceive a copyrighted work from an analog copy—the text of a literary work that is printed on a page of a book, or the image of a painting on a canvas. Digitally formatted works, though, can be perceived only by using a machine that converts the stored (and generally humanly imperceptible) data into images and/or sounds. A literary work on CD-ROM requires software and hardware to convert the data on the CD into readable text on a screen, just as a motion picture on DVD requires software and hardware to convert data on the disc into a series of related images and accompanying sounds. This process of converting digitally stored data into humanly perceptible images and sounds constitutes, in virtually all cases, the dis-

---

INFORMATION INFRASTRUCTURE TASK FORCE, INTELLECTUAL PROPERTY AND THE NATIONAL INFORMATION INFRASTRUCTURE: THE REPORT OF THE WORKING GROUP ON INTELLECTUAL PROPERTY RIGHTS 231 (1995) (second emphasis added). The drafters further stated that "if the circumvention device is primarily intended and used for legal purposes, such as fair use, the device would *not* violate the provision, because a device with such purposes and effects would fall under the 'authorized by law' exemption." *Id.* (empahsis original).

47. 17 U.S.C. § 1201(a)(3)(A).

48. *Id.* § 1201(b)(2)(A).

play or performance of the copyrighted work.[49] One displays a work whenever one "shows" a copy of the work using any device or process,[50] while any "rendering" of a work, or showing of its images in sequence, constitutes a performance.[51]

As a result, any access to a digitally stored work involves performing or displaying the work. In many instances, the performance or display made in the course of obtaining access to the work does not infringe on the exclusive rights of the copyright owner. Many such performances and displays are not public, and are therefore outside a copyright owner's exclusive rights of public performance and display.[52] As long as a user accesses the work in a place that is not open to the public, such as a home or hotel room, and where a substantial number of people is not gathered, the performance or display involved in accessing the work is not an act within the copyright owner's control.[53] Even displays in public places are outside the

---

49. In addition, in the view of some courts and commentators, any access to digitally stored information will, with current technology, involve reproducing the work in a copy, an activity within the copyright owner's exclusive § 106(1) right. In order for digitally stored data to be made visible or audible by a computer, the data must temporarily be stored in the computer's random-access memory ("RAM"). Some courts and commentators hold that temporary RAM storage constitutes the making of a "copy" or "phonorecord" for copyright purposes, and thus violates the copyright owner's reproduction right unless authorized or otherwise excused. *See, e.g.*, MAI Sys. Corp. v. Peak Computer, Inc., 991 F.2d 511, 518-521 (9th Cir. 1993). This view is sharply contested. *See, e.g.*, Reese, *supra* note 16, at 139 & n. 219. But if it is accepted, then any act of gaining access to a digitally stored work would involve an act of reproduction within the scope of the copyright owner's rights.

50. *See* 17 U.S.C. § 101 ("display"); *see also* H.R. REP. NO. 94-1476, at 64 (1976) ("In addition to the direct showings of a copy of a work, 'display' would include . . . the showing of an image on a cathode ray tube, or similar viewing apparatus connected with any sort of information storage and retrieval system."); Reese, *supra* note 16, at 86-88.

51. *See* 17 U.S.C. § 101 ("perform"); *see also* H.R. REP. NO. 94-1476, at 63 (1976). The House Report states:

> [A]ny individual is performing whenever he or she plays a phonorecord embodying the performance . . . . A performance may be accomplished 'either directly or by means of any device or process,' including all kinds of equipment for reproducing or amplifying sounds or visual images, . . . any type of electronic retrieval system, and any other techniques or systems not yet in use or even invented.

Id.

52. *See* 17 U.S.C. § 106(4)-(5).

53. *Id.* § 101 ("publicly"); *see also* Columbia Pictures Indus., Inc. v. Professional Real Estate Investors, Inc., 866 F.2d 278, 281-82 (9th Cir. 1989) (holding that viewing film on rented videodisc in hotel room videodisc player did not constitute public performance of film). This assumes that the user is not obtaining the access to the work by means of a transmission communicated from some other place, as transmissions to the public of performances or displays constitute public performances or displays.

scope of the copyright owner's right, as long as the display is made from a lawfully made copy and the viewers are present in the same place as that copy.[54]

Because accessing a digitally stored work requires performing or displaying that work, a technological protection measure that controls access to the work also controls the performance or display of that work. If § 1201(b) is read broadly so that a rights-control measure is protected against circumvention devices even when the measure is controlling performances or displays that are not within the copyright owner's rights, then a device that circumvents an access control is simultaneously a device that circumvents a rights control.[55] That reading would render the statute's careful distinctions between access controls and rights controls largely meaningless. For example, several statutory exemptions from the ban on devices that circumvent access controls would not, in practice, exempt any circumvention device, because even though such a device would be within an exemption from the access-control protections of § 1201(a)(2), the device would fall afoul of the rights-control protections of § 1201(b), to which the exemption does not apply.[56]

The legislative history of one particular exception from the anticircumvention bans further suggests that Congress did not consider an act of simply viewing or listening to a work to be within the rights of the copyright owner that could legally be protected by a rights-control measure. Section 1201(h) provides that in determining whether a device is a prohibited access-control circumvention technology, a court may consider the extent to which the device is necessary for preventing access by minors to material on the Internet. The legislative history of this section makes clear that it covers a device "which circumvents a technological protection measure effectively controlling access to a copyrighted work solely in order to provide a parent with the information necessary to ascertain whether

---

54. *See* 17 U.S.C. § 109(c); *see also* Reese, *supra* note 16, at 88-92. The public performance and display rights are also subject to a range of narrower, more specific exemptions, such as those allowing classroom performances and displays, and performances of nondramatic musical works in record stores. *See* 17 U.S.C. § 110(1), (7).

55. If the "RAM copy" doctrine, *see supra* note 49, is accepted, then a device that circumvents an access control will simultaneously be a device that circumvents a rights control because the device circumvents a control on the reproduction of the work by means of RAM storage, in addition to circumventing a control on the performance or display of the work.

56. Two statutory exemptions allowing in certain circumstances the making and use of devices that circumvent access controls, but not rights controls, are discussed in text accompanying notes 67-70, *infra*.

that material is appropriate for his or her child."[57] The drafters' careful explanation of the exemption's applicability only to access-control measures and not rights-control measures is illuminating:

> This provision is limited to the application of subsection (a) because the Committee does not anticipate that it would be necessary for parental empowerment tools to make copies of questionable material, or to distribute or perform it, in order to carry out their important function of assisting parents in guiding their children on the Internet. Accordingly, circumvention of copy controls, or of similar measures, should never be a necessary capability of a parental empowerment tool. By the same token, if a technology, product, service or device . . . (1) has the sole purpose of preventing the access of minors to certain materials on the Internet, and (2) . . . circumvents a technological protection measure that effectively controls access to a work as defined in subsection 1201(a)(3) only for the purpose of gaining access to the work . . . to ascertain whether it is suitable for a minor, but does not otherwise defeat any copy protection for that work, then that technology, product, service or device is only subject to challenge under subsection 1201(a)(2) and not subsection 1201(b). In such circumstances, no cause of action would lie under section 1201(b) and therefore limiting language would be unnecessary.[58]

In most cases, of course, a parent cannot "ascertain" whether a work is suitable for a minor without seeing or hearing that work, and making the work visible or audible is an act of performance or display. Nonetheless, the drafters quite clearly viewed a device that circumvents a control measure in order to make such a limited—and presumably private—performance or display as not within the scope of § 1201(b)'s ban on rights-control circumvention devices. This supports the view that a device that circumvents a technological control in order to allow uses of a work that are outside the control of the copyright owner, such as private performances or displays, is not a prohibited device under § 1201(b).

A prominent commentator, Professor Jane Ginsburg, has suggested that this more narrow reading of § 1201(b) may be what Congress intended, and that Congress offered broader protection under § 1201(a) specifically because of the narrowness of the protection of rights-control measures.[59] Professor Ginsburg considers the case of a consumer who has

57. S. REP. NO. 105-190, at 14 (1998).
58. *Id.*
59. *See* Ginsburg, *supra* note 12.

purchased a digital copy of a film protected by a technological measure that allows the film to be viewed only one time, and a device that allows the consumer to circumvent that measure and view the film repeatedly without any further payment to the copyright owner.[60] She notes that the consumer's viewing of the film would likely be a private performance:

> As a result, the user . . . might not contravene a "right of the copyright owner," and § 1201(b)['s ban on rights-control circumvention devices] might therefore be ineffective. By contrast, if each viewing is an act of "access" to the work, then, . . . [any unpaid viewings after the initial viewing would be achieved through] circumventing an access control, and would be in violation of § 1201(a).[61]

This suggests that Congress protected access-control measures at least in part because it believed that its protection for rights-control measures might not include controls that in part limit user activities outside the scope of the copyright owner's rights, such as private performances or displays.

If this more narrow reading of § 1201(b) is adopted by the courts, or even as long as uncertainty exists about how that subsection's anti-device provisions will be interpreted, copyright owners may see access-control measures as more desirable because of a greater degree of legal protection against circumvention devices. Section 1201(a) essentially outlaws devices that circumvent technological measures that control "access" to a work, rather than controlling the rights of the copyright owner. "Access" to a work, however, is not a defined term of particular scope, unlike the copyright owner's rights set forth in § 106. In addition, "access" to a work is not one of the rights granted in § 106, and is therefore not expressly limited by any of the provisions of §§ 107 through 122 as the § 106 rights are. While performing a film privately or in a classroom setting is entirely outside the scope of the copyright owner's rights to which § 1201(b) is directed, gaining access to the film in order to make such a performance is nowhere removed by statute from the scope of the copyright owner's ability to control access using measures protected by Chapter 12. Thus, as Professor Ginsburg noted:

> [T]he "access" that section 1201(a) protects goes beyond traditional copyright prerogatives. Indeed, the text indicates that "ac-

60. *Id.* at 143.
61. *Id.*

> cess" is distinct from a "right of the copyright owner under this title."
>
> . . . .
>
> . . . [I]n granting copyright owners a right to prevent circumvention of technological controls on "access," Congress may in effect have extended copyright to cover "use" of works of authorship . . . . In theory, copyright does not reach "use"; it prohibits unauthorized reproduction, adaptation, distribution, and public performance or display . . . . Not all "uses" correspond to these acts. But because "access" is a prerequisite to "use," by controlling the former, the copyright owner may well end up preventing or conditioning the latter.[62]

In keeping with this broad view of "access," courts have so far refused to read § 1201 in a way that treats as legitimate the circumvention of an access-control measure for the purpose of gaining access to a work in order to make noninfringing use of that work. In *Universal City Studios, Inc. v. Reimerdes*,[63] a case involving a computer program allowing the copying of encrypted motion pictures in DVD format, the district court considered whether "the possibility of noninfringing fair use by someone who gains access to a protected copyrighted work through a circumvention technology distributed by the defendants saves the defendants from liability [for dissemination of an access-control circumvention device] under Section 1201."[64] The court concluded that "nothing in Section 1201 . . . suggests"

---

62. *Id.* at 140, 143; *see also* Ginsburg, *supra* note 26, at 2 ("Every act of perception or of materialization of a digital copy requires a prior act of access. And if the copyright owner can control access, she can condition how a user apprehends the work, and whether a user may make any further copy."). Ginsburg states:

> [B]y purchasing [a] CD ROM, I have acquired lawful access to a *copy* of the work. . . . . But I do not access "the work" until I have entered the password (from the correct computer). Thus, when the law bars circumvention of controls on access to the "work", "access" becomes a repeated operation, whose controls will be substantially insulated from circumvention under the text of section 1201(a). I would therefore not be permitted to circumvent the access controls, even to perform acts that are lawful under the Copyright Act, such as using my copy in another computer or lending it to a friend . . . .

Ginsburg, *supra* note 12, at 140-41.

63. 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).

64. *Reimerdes*, 111 F. Supp. 2d at 323. While the court noted that the plaintiffs technically relied on both § 1201(a)(2) and § 1201(b)(1), the court's discussion of this issue focuses entirely on the § 1201(a) claim.

that result,[65] and held the defendants liable for violating § 1201(a)(2) by trafficking in a prohibited access-control circumvention device.

Chapter 12 may thus offer copyright owners more protection against circumvention technologies directed at access controls than at rights controls. At the very least, until the scope of protection available under § 1201(b) is clarified with respect to measures that control both uses reserved to the copyright owner and those uses that are entirely permitted by copyright law, copyright owners seeking the maximum legal protection available for their DRM technologies may have incentives to choose access-control measures over rights-control measures.

3. Rights Controls Are Subject to Fewer Exemptions but the Practical Impact of Such Exemptions Is Unclear

The anti-device provisions of Chapter 12 might be thought to offer somewhat stronger protection to rights controls than to access controls because the rights-control protections are subject to fewer express statutory exceptions. Chapter 12 provides several very detailed exemptions allowing development and employment of some circumvention technologies (and certain acts of circumvention). Two such exemptions apply to both access and rights controls.[66] But two other exemptions—those for encryption research and security testing—expressly allow development and use of devices that circumvent access controls, but not rights controls.[67] The statute, therefore, allows a somewhat broader scope for producing devices that circumvent access controls rather than rights controls. Thus, a copyright owner seeking maximum legal protection against circumvention

---

65. *Id*.

66. 17 U.S.C. § 1201(e) (exemption for law enforcement activities; applicable to "[t]his section"); *id.* § 1201(f)(2) (exemption for reverse engineering computer program in order to achieve interoperability; allowing development and employment of technological means of circumvention "[n]otwithstanding the provisions of subsections (a)(2) and (b)").

67. *Id*. § 1201(g)(4) (allowing development, use, and limited sharing of circumvention technologies "[n]othwithstanding the provisions of subsection (a)(2)"); *id*. § 1201(j)(4) (allowing development, production, distribution, or use of circumvention technologies "[n]othwithstanding the provisions of subsection (a)(2)"). Another provision that applies only to access controls, § 1201(h), discussed *supra* in text accompanying notes 57-58, is not actually an exemption, but rather a directive for a court to consider additional factors in determining whether a device is banned by § 1201 if the device includes a component that has the sole purpose of preventing access of minors to material on the internet. *See* Jonathan Band & Taro Issihiki, *The New Anti-Circumvention Provisions in the Copyright Act: A Flawed First Step*, CYBERSPACE LAW., Feb. 1999, at 2, 6; David Nimmer, *Puzzles of the Digital Millennium Copyright Act*, 46 J. COPR. SOC'Y 401, 408-409 (1999) ("This feature . . . in no way constitutes an exemption . . . .").

might prefer to use a rights control and thereby retain the ability to pursue legal action against the producer of a circumvention technology, even if that producer is engaged in otherwise statutorily acceptable encryption research or security testing.

It is unclear, however, whether allowing access-control circumvention devices for encryption research or security testing provides copyright owners with much practical incentive to prefer rights controls to access controls. The exceptions are quite narrowly defined.[68] The statute gives extremely detailed definitions as to what constitutes permissible encryption research and security testing and is designed to carefully limit the exemptions to persons engaged in those activities in good faith and not to others. In addition, the exemptions specifically prohibit any acts of security testing or encryption research that constitute copyright infringement.[69] Further, both exemptions fairly stringently limit the extent to which any circumvention technology developed for purposes of encryption testing or security research can be distributed to others.[70] Few devices or technologies are likely both to meet the exemptions' very specific standards and to be allowed to circulate freely under the exemptions. Given the relatively narrow scope of these exemptions to the ban on access-control circumvention devices, few copyright owners are likely to deploy rights-control measures, in whole or in part, out of a desire to avoid having their DRM technology subject to the exemptions.

B. Stronger Protection for Access Controls May Lead Owners to Prefer Them, Especially Since Access Controls May Easily Be Merged with Rights Controls

Because Chapter 12 protects access controls, but not rights controls, against acts of circumvention, and may offer access controls stronger protection against circumvention devices, copyright owners may have an incentive to prefer access controls over rights controls.[71] However, copy-

68. *See, e.g.*, Ginsburg, *supra* note 12, at 151 (describing "the proliferation of narrow exceptions" and noting "the overspecification of special exemptions"); Samuelson, *supra* note 2, 537-39 (describing "seven very specific exceptions" as "narrowly crafted").

69. 17 U.S.C. § 1201(g)(2)(D), (j)(2).

70. *Id.* § 1201(g)(4)(B) (allowing circumvention means to be provided "to another person with whom [the developer of those means] is working collaboratively for the purpose of conducting the acts of good faith encryption research"); *id.* § 1201(j)(4) (allowing distribution of circumvention means "for the sole purpose of performing the acts of security testing . . . provided such technological means does not otherwise violate section (a)(2)").

71. Indeed, the Register of Copyrights described the original bill that eventually became Chapter 12 as "providing stronger protection" to access controls than to rights controls. *WIPO Copyright Treaties Implementation Act; and Online Copyright Liability*

right owners who use rights controls may nevertheless be able to enjoy the stronger protection given to access controls. Copyright owners may deploy technological controls that aim to limit users' ability to reproduce or disseminate copyrighted works but that implement those limits by joining a rights-control mechanism with an access-control mechanism. Courts might find such a "merged" access and rights control entitled to the protection of § 1201(a) and § 1201(b), thus freeing copyright owners of the need to choose between the two.

Of the very few cases so far decided under Chapter 12, at least two have involved such hybrid access-and-rights-control measures.[72] The first, *RealNetworks, Inc. v. Streambox, Inc.*,[73] involved the plaintiff's "RealPlayer" software for receiving and performing streaming audio and video transmissions sent by computer servers using the company's

---

Limitation Act: Hearing on H.R. 2281 and H.R. 2280 Before the Subcomm. on Courts and Intell. Prop. of the House Comm. on the Judiciary, 105th Cong. 47 (1997) (statement of Marybeth Peters) [hereinafter Statement of Marybeth Peters].

72. At least eight cases involving claims under § 1201 have led to judicial opinions available in print or commercial electronic databases. *See* Pearl Invs. LLC v. Std. I/O, Inc., Civ. No. 02-50-P-H, 2003 U.S. Dist. LEXIS 5376 (D. Me. Apr. 2, 2003); Lexmark Int'l, Inc. v. Static Control Components, Inc., No. 02-571-KSF, 2003 U.S. Dist. LEXIS 3734 (E.D. Ky. Feb. 27, 2003); Portionpac Chem. Corp. v. Sanitech Sys., Inc., 210 F. Supp. 2d 1302 (M.D. Fla. 2002) (claim dismissed for failure to state a claim; no facts given as to the nature of the control measure involved); United States v. Elcom Ltd., 203 F. Supp. 2d 1111 (N.D. Cal. 2002); CSC Holdings, Inc. v. Greenleaf Elecs., Inc., No. 99 C 7249, 2000 U.S. Dist. LEXIS 7675 (N.D. Ill. June 1, 2000) (cable TV descrambler prohibited by § 1201(a)(2) and by 47 U.S.C. § 553); RealNetworks, Inc. v. Streambox, Inc., No. C99-2070P, 2000 U.S. Dist. LEXIS 1889 (W.D. Wash. January 18, 2000); 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); Sony Computer Entm't Am., Inc. v. GameMasters, 87 F. Supp. 2d 976 (N.D. Cal. 1999). In addition, claims under the anticircumvention provisions were made, but not considered by the court, in *Sony Computer Entertainment, Inc. v. Connectix Corp.*, 48 F. Supp. 2d 1212, 1223 (N.D. Cal. 1999), *rev'd*, 203 F.3d 596 (9th Cir. 2000).

Indeed, one of the few pre-DMCA copyright cases to involve technological protection measures concerned a control that could be described as a merged access-rights control. *Vault Corp. v. Quaid Software Ltd.*, 847 F.2d 255 (5th Cir. 1988), involved the plaintiff's software "designed to prevent the unauthorized duplication of [computer] programs." *Id.* at 256. The plaintiff's system sought to prevent such copying (an activity potentially within the copyright owner's rights) by a system that required a software manufacturer's original diskette copy of the software to be present in a computer's drive in order for the computer to run the software. *See id.* Thus, access to the copyrighted work—the computer program—was allowed only from the original copy sold by the copyright owner. By limiting access in this way, the system would make unauthorized copying of the work futile.

73. No. C99-2070P, 2000 U.S. Dist. LEXIS 1889 (W.D. Wash. Jan. 18, 2000).

RealServer" software.[74] A computer user who requested a transmission from a RealServer had to provide an authentication sequence, or "secret handshake," which was available only by using the RealPlayer software. By means of this authentication sequence, the transmitting RealServer would know that it was transmitting data to a RealPlayer and not to any other type of software.[75] All RealPlayer software, in turn, was designed to recognize and follow the instructions of the "copy switch" included in all RealServer transmissions. The copy switch indicated whether the receiving RealPlayer did or did not have permission to copy the transmitted audio or video by storing it, rather than simply playing the audio or video.[76] The defendant created a receiver for streaming transmissions, the Streambox VCR, that ignored the "copy switch" and allowed the user to record any received transmission. But in order for a Streambox VCR user to receive transmissions from a RealServer, the Streambox software had to provide the server with the "secret handshake" authentication sequence.[77]

The court treated the "secret handshake" as an access-control mechanism and the "copy switch" as a rights-control mechanism, and found that Streambox's product circumvented both measures, violating § 1201(a)(2) and § 1201(b).[78] However, both the handshake and the switch clearly seem to have been parts of a single technological system designed to prevent the *copying* of streaming transmissions, rather than actually to restrict *access* to the transmitted work (except as necessary to restrict copying). In order to make the rights-control measure effective, the system was designed to allow access to the work only by software known to respect the rights-control technology.[79]

---

74. *Id*. at *5.

75. *Id.* at *6 (Finding of Fact 12).

76. *Id.* at *6-7 (Finding of Fact 13).

77. *Id.* at *10-12 (Findings of Fact 23-26).

78. *Id.* at *18-20 (Conclusions of Law 7-9).

79. RealNetworks may have been interested in limiting access for a reason other than controlling copying. Allowing a particular audio or video transmission to be heard or seen only using RealPlayer software may give consumers an incentive to acquire a copy of the RealPlayer software, thus increasing RealNetwork's market share for media player software devices. As a practical matter, many transmitting entities make their audio or video files available in multiple formats so that users without RealPlayer software can hear or see the material using other software. It is not clear that copyright law, or "meta-copyright" law such as Chapter 12, should actively further a device-maker's attempts to increase the market share for its device by restricting users' ability to see or hear a copyrighted work on some other device. Indeed, copyright law has generally disfavored attempts by copyright owners of computer programs (such as RealPlayer) to use copyright law to limit the interoperability of their copyrighted computer programs with other computer programs or data. *See, e.g.*, Lotus Dev. Corp. v. Borland Int'l., Inc., 49 F.3d 807,

The federal litigation over the software known as "DeCSS" and the technological protection used with DVD films provides an even clearer example of merged access and rights controls.[80] The case involved an encryption program, the "Content Scramble System," or "CSS," used by motion picture studios to protect films distributed on DVD, and a challenge to the DeCSS computer software that circumvented CSS. The trial court described CSS as follows:

> CSS . . . is an access control and copy prevention system for DVDs developed by the motion picture companies . . . . It is an encryption-based system that requires the use of appropriately configured hardware such as a DVD player or a computer DVD drive to decrypt, unscramble and play back, but not copy, motion pictures on DVDs.[81]

CSS restricts copying of DVD films by joining an access-control measure with a rights-control measure. CSS allows a DVD film to be played, that is, accessed, only on a CSS-compliant player—the access-control measure.[82] And CSS-compliant players only allow a DVD film to be seen, not copied—the rights-control measure.[83]

As with the technology at issue in *RealNetworks*, CSS seems directed at controlling copying, not access. CSS imposes few actual limits on access,[84] in dramatic contrast to conventionally understood access-control

---

817-18 (1st Cir. 1995) (holding computer program's menu command hierarchy an uncopyrightable method of operation based in part on concerns about program compatibility); Sega Enters. Ltd. v. Accolade, Inc., 977 F.2d 1510, 1522-28 (9th Cir. 1992) (holding intermediate copying of a computer program as fair use where necessary to gain access to unprotected functional elements of program required for interoperability).

80. Universal City Studios, Inc. v. Reimerdes, 111 F. Supp. 2d 294 (S.D.N.Y. 2000).

81. *Id.* at 308.

82. *See id.* at 310 ("[O]nly players and drives containing the appropriate keys are able to decrypt DVD files and thereby play movies stored on DVDs.").

83. *Id.* (noting that CSS was licensed under strict security requirements "to ensure . . . that compliant devices could not be used to copy as well as merely play CSS-protected movies" and that CSS licensees "may not . . . make equipment that would supply digital output that could be used in copying protected DVDs"); *see also* Universal City Studios, Inc. v. Corley, 273 F.3d 429, 437 (2d Cir. 2001) ("With the [CSS] player keys and the algorithm, a DVD player can display the movie on a television or movie screen, but does not give a viewer the ability . . . to copy the movie.").

84. The main access limit imposed by CSS, which the courts in the DeCSS federal litigation never discussed, is that a user cannot, in some instances, access a DVD that is coded for a region other than the region of the user's DVD player. *See* Exemption to Prohibition on Circumvention of Copyright Protection Systems for Access Control Technologies, 65 Fed. Reg. 64,556, 64,569 (Oct. 27, 2000) (final rule adopting exemptions

measures, which impose far greater limits. For example, CSS does not tether playback of a particular copy of a film to a particular machine, thereby limiting access to the work to one particular DVD player. Similarly, CSS does not limit the time period in which a film can be viewed or the number of times it can be played. By contrast, the now-defunct Divx system typically allowed the owner of a copy of a film to play the film only on one system and only during one forty-eight-hour period, unless the user paid an additional fee for additional viewing.[85]

The real concern addressed by CSS was preventing users from *copying* films stored on DVD and *disseminating* those copies[86]—that is, from exercising exclusive rights of the copyright owners, the province of rights controls. As the trial court in the DeCSS litigation noted, "the principal focus of [the studios'] concern [over DeCSS] . . . is the transmission of pirated copies over the Internet or other networks."[87] The only real control that CSS placed on access was that users could access DVD films only on a CSS-compliant player, and the only reason to limit access to CSS-compliant players appears to be that those players prevented users from copying the films. Motion picture copyright owners seem to have little or no interest in restricting a user from *performing* a DVD film on a non-CSS-compliant player. As long as the user plays a lawfully made DVD,

---

from ban on acts circumventing access controls under § 1201(a)(1)(C)). Even this limit, though, is quite weak, as multi-region DVD players are available which allow the viewing of DVDs coded for different regions, as are players set to single, but non-U.S., region codes. *Id.*

85. The Divx system operated so that once a user began playback of a Divx disc, the disc could be played back only for a limited time (e.g., forty-eight hours) and only on players registered to the same billing account. In order to view the disc again, or on a different player, the user's player would have to contact the issuer of the disc and pay for additional access. *See, e.g.*, R. J. Dunill, *The Origins of the Original Divx*, *at* http://www.techtv.com/screensavers/answerstips/story/0,24330,3368584,00.html (modified Jan. 18, 2000).

86. Dissemination might be by distribution of copies of the film or by transmission of the film over computer networks such as the Internet, to recipients who could either view the transmitting performance or record a copy of the transmission.

87. Universal City Studios, Inc. v. Reimerdes, 111 F. Supp. 2d 294, 314 (S.D.N.Y. 2000); *see also* Universal City Studios, Inc. v. Corley, 273 F.3d 429, 436 (2d Cir. 2001) (noting that digital format carries risk that virtually perfect copies can be easily made and disseminated and that CSS was a response to this risk of increased piracy); *Reimerdes*, 111 F. Supp. 2d at 309 (noting film studios' concern that DVD technology carried "an increased risk of piracy by virtue of the fact that digital files . . . can be copied without degradation from generation to generation); *id.* at 315 (noting "two major implications" of DeCSS for studios, both stemming from ability of DeCSS users to reproduce and disseminate CSS-protected films); *id.* at 341-42 (discussing injury to plaintiffs from circulation of DeCSS and focusing on harm from use of DeCSS to make unauthorized copies).

the device on which she performs the film has no effect on the copyright owner.[88] The studios' real concern was to keep the user from using such a device to *copy* the film.[89]

CSS thus appears to be quintessentially a technological measure designed to protect rights of the copyright owner to reproduce and disseminate the film on a DVD. This control over the exercise of rights was implemented, however, by limiting access to the film only to certain devices. CSS allows a DVD to be played only on a licensed player, and licensed players do not provide digital output that can be copied.[90] Thus, the goal of limiting a user's ability to copy was achieved in part by restricting the user's ability to access the work by allowing access only on certain authorized devices. As a result, CSS could be seen as both a rights-control and an access-control measure within the definitions of Chapter 12, although in fact CSS primarily limits the reproduction of the protected work, rather than access to it.

The structure of merged access and rights controls seen in the DeCSS and *RealNetworks* cases is likely be used in the design of any "trusted system" that restricts a user's ability to copy (or distribute, perform, or display) copyrighted material. A trusted system consists of "hardware and software that can be relied on to follow certain rules [that] specify the cost and a series of terms and conditions under which a digital work can be used."[91] Key to a trusted system is that a work intended for restricted use is encoded "in such a way that it can be displayed or printed only by trusted machines."[92] Thus, a copyright owner who uses a trusted system to

88. *See Corley*, 273 F.3d at 453 ("The initial use of DeCSS to gain access to a DVD movie creates no loss to movie producers because the initial user must purchase the DVD.").

89. *See id.* ("However, once the DVD is purchased, DeCSS enables the initial user to copy the movie in digital form and transmit it instantly in virtually limitless quantity, thereby depriving the movie producer of sales.").

90. *See supra* note 83.

91. Mark Stefik, *Trusted Systems*, SCI. AM., March 1997, at 79; *see also* COMPUTER SCI. & TELECOMM. BD., NAT'L RESEARCH COUNCIL, THE DIGITAL DILEMMA 167-71 (2000).

92. Stefik, *supra* note 91, at 79; *see also id.* at 80 (describing transaction on trusted system to acquire a digital copy of a book and noting that "[t]he entire transaction . . . is preceded by an exchange of information in which the seller ensures that [the buyer's] machine is a trusted system"); Mark Stefik, *Shifting the Possible: How Trusted Systems and Digital Property Rights Challenge Us to Rethink Digital Publishing*, 12 BERKELEY TECH. L.J. 137, 139-40 (1997) (describing that before online trusted-system transaction can take place between distributor and consumer, "the two systems—the consumer's system and the distributor's system—need to establish that they are both trusted systems"); Mark Stefik & Alex Silverman, *The Bit and the Pendulum: Balancing the Interests of*

control a user's ability to exercise rights reserved to the copyright owner will use both an access control—technology allowing the user to view, hear, store, or print the work only on compliant devices—and a rights control—technology in those compliant devices restricting the user's copying, performance, etc., of the work. Therefore when using such trusted systems, copyright owners could be seen as using both an access-control measure *and* a rights-control measure.

If a merged access and rights control such as a trusted system is viewed by courts as both an access and a rights control, copyright owners using such a system may simultaneously enjoy the different legal protections afforded to each type. The DeCSS litigation suggests precisely this outcome. Although the copyright owners were concerned about DeCSS because of its potential to allow users to make copies of films stored on DVD (and to transmit those copies over computer networks), the district court ruled based on its legal analysis that DeCSS was a prohibited device for circumventing an *access* control, not based on an analysis of DeCSS as a technology for circumventing a copy control.[93] This is not to say that the result in *Reimerdes* would have been any different if the court had analyzed CSS as a rights control, rather than an access control. After all, the *device* bans of § 1201 are virtually identical, so that a device that circumvents a trusted system seems likely in many cases to be prohibited, whether it is viewed as a device to circumvent an access-control or a rights-control measure. Indeed, it is quite likely that the courts would have found DeCSS to be a rights-control circumvention technology prohibited under § 1201(b)(1) and provided the same relief to the plaintiffs. But by basing their decisions about a control measure directed at preventing copying and dissemination almost wholly on the grounds that DeCSS was an improper access-control circumvention device, the courts' decisions suggest that trusted systems and similar merged access and rights controls will enjoy both the statutory protections given to rights controls *and* the apparently stronger protections afforded access controls where the treatment of the two types differs, such as for acts of circumvention.

This approach to merged control measures is not necessarily dictated by the statute. While the *RealNetworks* and *Reimerdes* courts viewed merged technological controls as constituting an access control protected under § 1201, a future court might read the definition of an access-control

---

Stakeholders in Digital Publishing, COMPUTER LAW., Jan. 1999, at 1, 4 ("Trusted systems . . . exchange copies of the work only with systems that can prove themselves trusted via challenge-response protocols.").

93. *See* Universal City Studios, Inc. v. Reimerdes, 111 F. Supp. 2d 294, 316-24 (S.D.N.Y. 2000).

measure to exclude merged access and rights controls that in fact serve principally to control reproduction and dissemination, rather than access. The key phrase in this reading of the definition of a protected access-control measure is that the measure must control access "in the ordinary course of its operation."[94] As the Register of Copyrights noted in testimony to Congress, this definition would not cover "every technological measure that controls access."[95] Rather, the "'ordinary course of its operation' [language] would exclude technologies that may have the incidental or unintended effect of controlling access, or do so only when used in an unusual way."[96] Thus, a court might decide that the RealNetworks and CSS technological protection systems control access only incidentally because their control over access is merely incidental to the systems' control over a user's ability to reproduce protected works. Nonetheless, given the decisions to date interpreting Chapter 12, and the tendency of the courts rendering those decisions to read the statute fairly broadly, it is more likely that courts will continue to consider the access-control portion of a merged access and rights control to constitute an access control protected against circumvention by § 1201(a).

Copyright owners interested in controlling the exercise of their rights under § 106 may thus have incentives to deploy merged technological measures. These merged measures would control a user's activities in part by allowing access to the work only via certain devices. These devices would then restrict the user's ability to copy, disseminate, perform, or display the work. By doing this, the copyright owner would be able to protect the technological measure as both an access control *and* a rights control. Since access controls, as discussed above, enjoy stronger protection than rights controls under Chapter 12, copyright owners seeking maximum protection for their rights-controlling technological protection systems might well decide to deploy merged controls.

III. IMPACT ON USERS OF COPYRIGHTED WORKS IF COPYRIGHT OWNERS DEPLOY MERGED CONTROL MEASURES

As suggested in Part II, copyright owners may adopt DRM technologies that restrict *copying* by limiting *access* to authorized devices, so that the technology simultaneously qualifies both as an access control and a

94. 17 U.S.C. § 1201(a)(3)(B) (2000).

95. Statement of Marybeth Peters, *supra* note 71, at 47.

96. *Id.* (commenting on definitional language in its initial appearance in introduced legislation).

rights control. This use of merged access and rights controls, may, however, undermine Chapter 12's carefully differentiated treatment of the two types of controls. Understanding why this result is problematic requires understanding why the statute allows circumvention of rights-control measures in the first place.

Congress chose not to prohibit circumvention of rights-control measures in order to accommodate copyright owners' need to protect against infringement of their works in digital format and the need to allow the public to continue to make noninfringing uses of copyrighted works.[97] This emerges very clearly in the Register of Copyright's statement to Congress evaluating the initial draft of the provisions that eventually became Chapter 12.[98] The Register pointed out how the bill would accommodate the public's ability to engage in noninfringing uses:[99]

> The Copyright Office firmly believes that the fair use doctrine is a fundamental element of the copyright law, and that its continuing role in striking an appropriate balance of rights and exceptions should not be diminished. We also believe that it is possible to provide effective protection against circumvention without undermining this goal.
>
> Section 1201 seeks to accomplish this result in several ways. First, it treats access-prevention technology separately from infringement-prevention technology, and does not contain a prohibition against individual acts of circumvention of the latter. As a

97. *See* United States v. Elcom Ltd., 203 F. Supp. 2d 1111, 1120 (N.D. Cal. 2002) ("Congress did not prohibit the act of circumvention [of rights controls] because it sought to preserve the fair use rights of persons who had lawfully acquired a work."); Band & Issihiki, *supra* note 67, at 3 ("The Administration [while formulating its legislative proposal for the anticircumvention bill] eliminated [a draft ban on acts of circumventing rights controls] in response to the library and education communities' concerns about the negative impact of the legislation on fair use."); David Nimmer, *Appreciating Legislative History: The Sweet and Sour Spots of the DMCA's Commentary*, 23 CARDOZO L. REV. 909, 932, 984-85 (2002) (noting that structure of § 1201 allows § 1201(b) to encompass fair use).

98. *See* Statement of Marybeth Peters, *supra* note 71.

99. While there are substantial differences between the bill about which the Register testified and the full text of Chapter 12, the enacted law made few if any changes to the fundamental features contained in the initial bill, particularly in the definitions of the measures protected, the prohibitions imposed, and the structure of differentiating between access controls and rights controls and not barring acts of circumvention of the latter. *See* Band & Issihiki, *supra* note 67, at 3 (noting that the basic framework of initial 1997 administration proposals of § 1201 "endures in the legislation enacted by Congress"); Nimmer, *supra* note 97, at 921 (noting that initial bill's "tripartite scheme survived through enactment").

> result, an individual would not be able to circumvent in order to gain unauthorized access to a work, but would be able to do so in order to make a fair use of a work which she has lawfully acquired.[100]

Register Peters' last sentence is repeated almost verbatim in the House Judiciary Committee's report on the DMCA.[101] The Copyright Office has officially expressed the same view on the enacted Chapter 12, stating, "The decision not to prohibit the conduct of circumventing [rights] controls was made, in part, because it would penalize some noninfringing conduct, such as fair use."[102]

The Chair of the House Judiciary's subcommittee on intellectual property, Rep. Howard Coble—an initial sponsor of the anticircumvention legislation and a guiding force in its adoption—echoed these views in a letter to two colleagues, Rep. Tom Campbell and Rep. Rick Boucher, introduced into the *Congressional Record* during the floor debate leading to initial House passage of the anticircumvention provisions.[103] Campbell and Boucher had introduced a competing bill that they asserted better balanced copyright owners' needs for protection with the public interest in noninfringing uses.[104] Coble's letter explains his belief that the provisions eventually adopted as Chapter 12 offer substantial protection for noninfringing uses, and points principally to the lack of a ban on acts of circumventing rights-control measures as a key safeguard for such uses:

> As it was introduced, H.R. 2281 contained two important safeguards for fair use. First, the bill dealt separately with technological measures that prevent access and technological measures that prevent copying. As to the latter, the bill contained no pro-

100. Statement of Marybeth Peters, *supra* note 71, at 49. Register Peters noted that she was using "fair use" to refer collectively to "all permitted uses under the Copyright Act, including those made possible by the idea-expression dichotomy and the first sale doctrine." *Id.* at 48, n.1.

101. *See* H.R. REP. NO. 105-551, pt. 1, at 18 (1998) ("[A]n individual would not be able to circumvent in order to gain unauthorized access to a work, but would be able to do so in order to make fair use of a work which he or she has acquired lawfully.").

102. Exemption to Prohibition on Circumvention of Copyright Protection Systems for Access Control Technologies, 65 Fed. Reg. 64,556, 64,557 (Oct. 27, 2000).

103. This version passed in the House did not differ in any relevant respect from the bill approved by the Senate, and from the bill produced by the conference committee and enacted by Congress.

104. H.R. 3048, 105th Cong. (1997).

> hibition on the act of circumvention itself, leaving users free to circumvent such measures in order to make fair use copies.[105]

Again, the absence of penalties for circumventing rights-control measures was recognized as a key feature of the legislation and as a mechanism for preserving fair use and other noninfringing uses of copyrighted works.

Thus, as Professor Pam Samuelson has concluded, "[t]he text of the DMCA and its legislative history clearly demonstrate that Congress intended to ensure that users would continue to enjoy a wide range of noninfringing uses of copyrighted works, even if copyright owners used technical protection systems to impede them."[106] One of the principal ways Congress implemented that intent was by expressly declining to prohibit acts that circumvent rights-control measures. Instead, Congress left regulation of that activity to the provisions of copyright law, which target only infringing activity.

In this context, both the deployment of merged access and rights controls and courts' treatment of such a merged control measure as protected simultaneously under § 1201(a) and § 1201(b) raise troubling questions about the statute's ability to preserve noninfringing uses of technologically protected works by not banning the act of circumventing a rights control. Users facing merged access and rights controls may be unable to circumvent the rights control (an entirely legal activity if the user's post-circumvention use is not infringing) without circumventing the access

---

105. 144 CONG. REC. H7096-98 (daily ed. Aug. 4, 1998) (letter of Rep. Coble, Chair, Subcomm. on Courts and Intellectual Prop., House Judiciary Comm., to Rep. Campbell and Rep. Boucher (June 16, 1988)); *see also* H.R. REP. NO. 105-551, pt. 1, at 18 (1998). The Report states:

> Paragraph (a)(1) does not apply to the subsequent actions of a person once he or she has obtained authorized access to a copy of a work protected under Title 17, even if such actions involve circumvention of additional forms of technological protection measures. In a fact situation where the access is authorized, the traditional defenses to copyright infringement, including fair use, would be fully applicable. So, an individual would not be able to circumvent in order to gain unauthorized access to a work, but would be able to do so in order to make fair use of a work which he or she has acquired lawfully.

Id. The second safeguard Coble pointed to was § 1201(c), which provides that nothing in § 1201 "shall affect rights, remedies, limitations, or defenses to copyright infringement, including fair use, under this title." 144 CONG. REC. H7097 (daily ed. Aug. 4, 1998) (letter of Rep. Coble, Chair, Subcomm. on Courts and Intellectual Prop., House Judiciary Comm., to Rep. Campbell and Rep. Boucher (June 16, 1988)).

106. Samuelson, *supra* note 2, at 546.

control (a prohibited activity).[107] As a practical matter, then, the deployment of merged controls may restrict or eliminate users' ability to legally circumvent rights controls. This undercuts the congressional intent in drafting the DMCA expressly to allow circumvention of rights controls so long as the circumventor does not engage in copyright infringement. If merged control measures are widely adopted, and if circumventing a merged control is treated as circumventing an access control, such treatment will suck most of the oxygen out of Chapter 12's breathing space for circumvention of rights-control measures for noninfringing purposes.[108] As Professor Pam Samuelson suggests in a related context, "this presents

107. Perhaps not all circumvention of a merged control will require circumvention of both the access-control and rights-control aspects of the system. Users might, for example, access the work on an "approved" or "trusted" device (e.g., an actual RealPlayer computer program, or a CSS-compliant DVD player), but adjust that device so that it does not respect the rights-control rules that it would ordinarily implement. A court might well find, though, that accessing a work on an altered device constitutes circumvention of an access control. For example, a court might find that CSS restricts access to CSS-compliant players, and that a DVD player that was CSS-compliant when produced by the manufacturer but that has been altered to allow the recording of digital output is no longer a CSS-compliant device. As a result, gaining access to a DVD film using the altered player could be considered circumventing the access-control aspect of CSS just as much as gaining access to the film using a player that was noncompliant *ab initio* would be. Even if such a process were not considered as circumvention of an access control, merged controls may still be problematic for the goal of allowing noninfringing circumvention. Given the limited number of users likely to be technologically sophisticated enough to engage in acts of circumvention without a device provided by someone else, it is not clear that Chapter 12 should make noninfringing circumvention more difficult by prohibiting the user from engaging in one likely avenue of circumvention, in this case the possibility of deceiving the control system into believing that the user's device will comply with the system's rights-control rules.

108. The impact of merged controls might be less significant if courts interpret Chapter 12's anticircumvention provisions to allow some circumvention of access controls in order for the circumventor to make fair use or other noninfringing use of the protected work. Both Pam Samuelson and Jane Ginsburg have suggested that the statute should be so interpreted. *See* Jane C. Ginsburg, *Copyright Use and Excuse on the Internet*, 24 COLUM.-VLA J.L. & THE ARTS 1, 8-9 (2000) ("[O]ne might conclude that courts may—given an appropriate fact situation—apply [the fair use doctrine] to § 1201(a) by articulating additional, and highly contextual, limitations on the prohibition on circumvention of access controls."); Samuelson, *supra* note 2, at 539-40, 545-46. So far, however, courts have generally not followed this interpretive path, at least with respect to Chapter 12's device bans. *See* United States v. Elcom Ltd., 203 F. Supp. 2d 1111, 1123-25 (N.D. Cal. 2002); Universal City Studios, Inc. v. Reimerdes, 111 F. Supp. 2d 294, 322-24 (S.D.N.Y. 2000) (finding no fair use limitation on anticircumvention provisions). *But see* RealNetworks, Inc. v. Streambox, Inc., 2000 U.S. Dist. LEXIS 1889 (W.D. Wash. 2000) (finding no fair use on the facts of the case, but not rejecting the possibility of fair use out of hand).

the question of whether Congress should be understood to have made an empty promise of fair use and other privileged circumvention."[109]

The Copyright Office noted this problem in its first rulemaking on exemptions from the circumvention ban, stating that "[t]he merger of technological measures that protect access and copying does not appear to have been anticipated by Congress."[110] The Office pointed out that "the merger of access and use controls would effectively bootstrap the legal prohibition against circumvention of access controls to include copy controls and thereby prevent a user from making otherwise noninfringing uses of lawfully acquired copies."[111] Therefore, the Copyright Office said, "the implementation of merged technological measures arguably would undermine Congress's decision to offer disparate treatment for access controls and use controls in section 1201."[112]

If copyright owners deploy merged control measures, and if courts protect those controls as both access and rights controls, then the freedom that Chapter 12 allows for circumventing rights controls will not, in fact, be the freedom to make noninfringing uses of technologically protected works as Congress intended it to be. A more careful treatment of merged controls under Chapter 12 is required.

IV. POSSIBLE RESPONSES

Part II suggested that § 1201 may give copyright owners an incentive to adopt DRM systems combining an access control with a rights control, in an attempt to secure the maximum legal protection possible for their system. Part III suggested that such merged control measures, at least as they have been treated to date by courts applying § 1201, undermine a critical congressional goal behind that section: permitting some circumvention of technological protection systems to allow noninfringing uses. This Part considers what responses might be appropriate.

A. Do Nothing

Perhaps the likely deployment of merged access and rights controls requires no response. One reason why no response might be needed is that users may continue to be able to make noninfringing uses of copyrighted

109. Samuelson, *supra* note 2, at 557.

110. Exemption to Prohibition on Circumvention of Copyright Protection Systems for Access Control Technologies, 65 Fed. Reg. 64,556, 64,568 (Oct. 27, 2000) (also noting that "neither the language of section 1201 nor the legislative history addresses the possibility of access controls that also restrict use").

111. *Id*.

112. *Id*.

works in analog format. Many copyrighted works today continue to be widely available in both protected digital and unprotected analog formats, so that those who wish to make noninfringing uses of the work can do so by acquiring an unprotected analog copy. Motion pictures, for example, are today often available both on DVD, protected by CSS, and on videocassette, unprotected by CSS, perhaps alleviating some concerns about the difficulty a consumer might have in circumventing CSS to engage in noninfringing use of a film that she owns on DVD. In addition, even with protected digital copies, copying of the work may be possible when it is made audible or visible. As the Second Circuit noted in *Corley*, a user could play a film on a CSS-protected DVD and "recor[d] portions of the video images and sounds . . . by pointing a camera, a camcorder, or microphone at a monitor as it displays the DVD movie."[113] But relying on analog copying to preserve consumers' ability to make noninfringing uses raises several problems. In the case of many works, copyright owners may well be moving toward issuing works only in protected formats, ending the availability of new works in unprotected analog copies. And while the possibility of copying the visual or audio output of a protected work may offer some room for noninfringing use, it seems likely as a practical matter to substantially diminish the quality and availability of such use. In addition, some copyright owners have expressed a desire to use technology, perhaps backed by legal requirements, to "plug the analog hole" and prevent such copying of copyrighted works.[114]

A more significant reason why merged access and rights controls might not require any adjustment of Chapter 12's legal protections is that the law already prohibits circumvention devices for both types of controls. The main difference in the regulation of access and rights controls, which merged control measures threaten to blur, is that the statute bans only *acts* that circumvent access-control measures. Circumvention *devices*, on the other hand, are equally prohibited, regardless of which type of control measure they circumvent. As a result, the ban on acts of circumvention may be relatively unimportant as a practical matter, as all of the "action" may involve circumvention devices, for several reasons.[115]

---

113. Universal City Studios, Inc. v. Corley, 273 F.3d 429, 459 (2d Cir. 2001).

114. *See, e.g.*, Motion Picture Ass'n of Am., *Content Protection Status Report*, at 9, *at* http://judiciary.senate.gov/special/content_protection.pdf (Apr. 25, 2002).

115. As Pam Samuelson has noted, "the anti-device provisions are, as a practical matter, by far the more important rules." Samuelson, *supra* note 2, at 554; *see also* Yochai Benkler, *Free As the Air to Common Use: First Amendment Constraints on Enclosure of the Public Domain*, 74 N.Y.U. L. REV. 354, 416 (1999).

First, any circumvention of most effective access controls will likely require technological ability beyond that of the average copyright consumer.[116] Few DVD owners can defeat CSS on their own, without a device supplied by someone of greater technical skill.[117] One court even suggested that Congress intended "to leave technologically unsophisticated persons who wish to make fair use of encrypted copyrighted works without the technical means of doing so."[118] Second, as noted above,[119] even if an ordinary consumer obtains a circumvention device, any of her private acts of circumvention not resulting in subsequent—and independently actionable—acts of copyright infringement are unlikely to come to the attention of a copyright owner and result in enforcement efforts against her. On the whole, so few people may be able to circumvent access controls without the aid of prohibited circumvention technologies, and so few uses of those prohibited technologies are likely to be detectable, that copyright owners may get almost all of the practical protection they need and want

116. *See, e.g.*, Benkler, *supra* note 115, at 416 ("Even if a few savvy users can circumvent without relying on the products or services of others, the vast majority of users will have to rely on such products or services."); David Nimmer, *A Riff on Fair Use in the Digital Millennium Copyright Act*, 148 U. PA. L. REV. 673, 733, 739-40 (2000) (noting that "users . . . who lack technical expertise . . . are effectively checkmated" by Chapter 12's statutory scheme); Samuelson, *supra* note 2, at 551 ("It is unclear whether Congress intended for the technologically savvy who could 'do it themselves' to be the only ones who could engage in privileged acts of circumvention."). On the other hand, some protection systems *might* be easily circumvented. One protection system for recorded music distributed on CD in Europe was designed to prevent the CD from being played in a computer, as opposed to a single-purpose music CD player, such as a Discman or a stereo component, thus limiting access to certain types of devices. Reportedly, however, the protection system could be defeated by drawing a line with a black magic marker on the surface of the disc around the outer edge. If the access control qualified as "effectively" protecting access and thus covered by § 1201(a), even the technologically unsophisticated would be able to circumvent the access control in violation of § 1201(a)(1), though again copyright owners would seem unlikely to be able to detect any significant number of instances of prohibited circumvention.

117. Indeed, even with the source code for various programs to defeat CSS circulating fairly freely in a variety of forms, including on t-shirts and business cards, most consumers seem unlikely to be able to use that source code to actually decrypt and copy a film on a DVD. *See also* Benkler, *supra* note 115, at 416 (noting that barring circumvention technologies will "by and large negate the possibility of circumvention" as effectively as barring sale of VCRs would prevent most home copying of television broadcasts).

118. Universal City Studios, Inc. v. Reimerdes, 111 F. Supp. 2d 294, 324 (S.D.N.Y. 2000); *see also* Nimmer, *supra* note 116, at 739 (arguing that Congress's failure to allow the technologically unskilled noninfringing circumventor to acquire circumvention technology "seems to be a conscious contraction of user rights").

119. *See supra* notes 18-20 and accompanying text.

from the device bans. Indeed, during the process leading to the enactment of Chapter 12, copyright owners strongly resisted proposals to adopt only a ban on acts of circumvention, arguing that they needed protection against the circulation of devices because of the difficulty of enforcing an act ban.[120]

For most consumers, then, the absence of a ban on the circumvention of rights-control measures is of little or no practical import. Most users do not have the technological know-how to engage in legal circumvention of a rights control without the assistance of a circumvention technology. But because the device ban of § 1201(b) prohibits the manufacture and distribution of such circumvention technologies, few consumers will likely obtain circumvention technologies.[121] Therefore, few consumers will be able

---

120. *See, e.g.*, Band & Issihiki, *supra* note 67, at 3-4 (noting copyright owners' resistance to alternative legislative proposal that focused only on acts of circumvention, not devices, because of fear that anticircumvention ban would be too difficult to enforce if devices were available to consumers); Samuelson, *supra* note 2, at 554-56 (noting that administration proposals focused on device bans from the beginning and that proponents testified before Congress that anti-device provisions were "needed to stop deliberate and systematic piracy by 'black box' providers").

121. A consumer capable of building her own circumvention device might not, however, violate the device ban in doing so. Section 1201 does not allow anyone to "manufacture, import, offer to the public, provide, or otherwise traffic in" any prohibited circumvention technology. 17 U.S.C. § 1201(a)(2), (b)(1) (2000). Provided that the device builder uses the device only for her own acts of circumvention, she would not be offering the device to the public or providing or otherwise trafficking in it, and if she builds it herself in the U.S., she would not be importing it. Thus, the only liability she might face would be for the "manufacture" of the device. But if she makes only the device or devices she needs for her own use, she arguably is not engaged in the "manufacture" of the device. While "manufacture" does mean to make a finished product, it typically means to do so in some quantity. I might build a bookshelf for my home, or sew several shirts to wear, or bake a loaf of bread every week, but it would be odd to say that I am "manufacturing" bookshelves or shirts or bread. In addition, it is clear from the legislative history that the device bans in § 1201 were designed to prevent large-scale circumvention and to penalize those who would assist others in circumventing activities. As Register Peters stated:

> Because of the difficulty involved in discovering and obtaining meaningful relief from individuals who engage in acts of circumvention, a broader prohibition extending to those *in the business* of providing the means for circumvention appears to be necessary to make the protection adequate and effective [as required by treaty]. It is the conduct of *commercial suppliers* that will enable and result in large-scale circumvention.

Statement of Marybeth Peters, *supra* note 71, at 48 (emphasis added); *see also* Samuelson, *supra* note 2, at 555 (noting that proponents testified before Congress that anti-device provisions were "needed to stop deliberate and systematic piracy by 'black box' providers"). Thus, someone who produces a single circumvention device for her

to engage in noninfringing acts of circumvention, even though the copyright law allows such acts. While a copyright owner's use of a merged control may interfere with a consumer's ability to legally circumvent the rights-control portion of the merged control, this interference will have little practical impact, since so few consumers will be able to engage in legal circumvention of rights controls in any event. From this perspective, deployment of merged access and rights controls and enforcement of the ban on acts that circumvent access controls will not practically hinder many legal acts of circumventing rights controls, because there may be few such acts.

In some instances, though, acts that circumvent merged control measures may not require illegal circumvention devices[122] and may come to the attention of copyright owners through subsequent acts of the circumventor. In some instances the circumventing party will not have committed any subsequent act of copyright infringement, because her use of the work at issue was allowed by copyright law.[123] One example is someone who circumvents a technological control measure in order to copy parts of a work to make a parody or other noninfringing transformative fair use. The copier is not liable for copyright infringement for her copying, nor is she liable for circumventing a rights-control measure in order to make the copy because copyright law allows her use of the work.[124] But if the rights-control measure was part of a merged access and rights control, she might face liability for violating § 1201(a)(1) because she has probably circumvented the access control as well as the rights control. In this instance, enforcing the act ban is inconsistent with the statute's refusal to impose liability on the copier for circumventing a rights control in order to engage in noninfringing activity. Thus, if Congress was serious about exempting acts circumventing rights controls from liability in order to allow noninfringing uses, merged control measures will require statutory adjustments.

---

own use might well not be violating the device bans, and if she used the device to circumvent a rights control and make a noninfringing use of the protected work, she would face no legal liability whatsoever. That result seems entirely in line with the express congressional intent of preserving consumers' ability to make noninfringing uses.

122. As discussed in Part II.A.2 above, devices that circumvent a technological measure that both protects a right of the copyright owner and prevents noninfringing uses might not be an illegal circumvention device.

123. *See supra* notes 15-17 and accompanying text.

124. *See supra* notes 15-17 and accompanying text.

B. Permit Acts Circumventing Access Controls *If* Purpose Is to Engage in Noninfringing Use

Congress apparently thought that by not restricting acts circumventing rights-control measures, noninfringing uses of copyrighted works would continue even as copyright owners deploy legally protected technological protection measures. However, protecting merged control measures as both access and rights controls may thwart this plan. To effectuate the congressional intent to allow noninfringing circumvention, an exemption from § 1201(a)(1)'s ban on circumventing acts might be needed.

The simplest way to allow circumvention of merged control measures for noninfringing purposes is to tie liability under § 1201(a)(1) in such situations to copyright infringement. If someone circumventing a merged access and rights control would not be liable for copyright infringement, then she would also not be liable under § 1201(a)(1) for circumventing the access control, just as she would not be liable under § 1201(b) for circumventing the rights control. Congress could add such an exemption to § 1201.

Not only does such an exemption protect the breathing space that Congress allowed for noninfringing circumvention, it also would not necessarily have a significant undue impact on Chapter 12's overall level of legal protection for copyright owners' use of technological protection measures. This exemption would not apply to the device ban of § 1201(a)(2).[125] As a result, those wanting to circumvent merged control measures for noninfringing purposes would have to either be sufficiently technologically savvy to create their own device or acquire a circumventing device. If such a device may be legally manufactured and distributed

125. This is not to suggest that the device bans in Chapter 12 are not themselves problematic. As many commentators have noted, the breadth of those bans may mean that very few people—the highly technologically skilled—will in practice be able to engage in the specifically permitted acts of circumvention, since the vast majority of those who might want to engage in such circumvention will not be able to do so without acquiring technology from someone else. *See, e.g.*, Band & Issihiki, *supra* note 67, at 6 (noting that exception allowing circumvention to protect personally identifying information does not apply to device bans and therefore "[i]t is not clear how users are expected to effectuate [permitted] circumvention if developers are not permitted to manufacture and distribute circumvention devices"); Burk & Cohen, *supra* note 32, at 49-50 ("As a practical matter . . . any exemptions ultimately declared [by the Librarian of Congress] will have very limited utility; self-evidently, most users will be unable to exercise their circumvention rights unless they are provided with the tools to do so."); Samuelson, *supra* note 2, at 551. Any more general reworking of the device bans should, of course, take into account the problem of merged controls, but the problems of the device bans generally are beyond the scope of this Article.

under § 1201(a)(2), then not penalizing those who use the device for noninfringing purposes is unlikely to seriously undermine § 1201(a)(1)'s protection of the copyright owner. Indeed, as a practical matter, detection of dispersed, private circumventing uses of the device—whether those uses are legal or illegal—will likely remain difficult. By contrast, if the device violates § 1201(a)(2), then those who manufacture or traffic in the device would be subject to liability. Exempting from liability those users who use the illegal device for noninfringing purposes is unlikely to significantly hamper enforcement against device manufacturers and traffickers. Congress included the anti-device provisions, after all, because enforcement against individual users was perceived as more difficult than against those supplying circumvention technologies.

The fact that some additional acts of circumvention—circumvention of merged control measures for noninfringing purposes—would be allowed under § 1201(a)(1) also does not necessarily affect the circumvention device ban under § 1201(a)(2). Devices are prohibited if they are "primarily designed or produced for the purpose of circumventing" an access-control measure or if they have "only limited commercially significant purpose or use other than" such circumvention.[126] If noninfringing circumvention of merged control measures is allowed, a greater number of uses of a circumvention device may be permitted. Those uses, however, would still be circumventing uses. The device bans do not bar technologies that have limited commercially significant purpose or use other than engaging in *prohibited* circumvention of an access control. The statutory language suggests that even permitted circumvention will not count in favor of a device in determining the device's primary purpose or commercially significant uses. The key issue under the statute is whether the purpose and use of the technology is to circumvent an access-control measure, not whether such circumvention is allowed.[127] A device that has a commercially significant purpose of making statutorily permitted circumvention of an access-control measure (such as circumvention to protect personally identifying information[128]) is still a device without a commercially signifi-

126. 17 U.S.C. § 1201(a)(2)(A)-(B) (2000).

127. Indeed, there might otherwise be little need for the specific exemptions from the device bans in § 1201(a) and § 1201(b), since devices needed for exempted acts of circumvention for purposes of reverse engineering, security testing, and encryption research would have purposes other than *prohibited* circumvention: they could be used for *permitted* circumvention.

128. 17 U.S.C. § 1201(i).

cant purpose other than circumventing an access control, and thus likely prohibited under § 1201(a)(2).[129]

A final concern raised by such an exemption might be that some circumvention, even of merged control measures, should remain prohibited. While merged controls may be aimed largely at limiting copying or dissemination of the protected work, as in *RealNetworks* and *Reimerdes*, they might actually be intended to control access to copyrighted works independently of their control on copying. For example, a trusted system might allow a user to purchase a digital copy of a motion picture for two different prices, one price for a copy without any restrictions on use (other than those imposed by copyright law) and a lower price for a copy that may be played only for a twenty-four-hour period during the first thirty days after the copy is purchased. This would be a quintessential access control system. As Jane Ginsburg has explained, "In theory, access controls are designed to protect a business model based on price discrimination according to intensity of use."[130] If a merged control measure is in fact aimed substantially at controlling access, then an exemption allowing a user to circumvent a merged control whenever the user's post-circumvention use is noninfringing may be too broad. For instance, someone who buys a time-limited copy of a copyrighted work and then circumvents the access control in order to view the work privately after the time limit has expired would probably be covered by the exemption, since the post-circumvention private performance of the work would not be a copyright infringement. It is unclear, however, that circumvention of the merged control measure for this purpose should be allowed.

Thus, an exemption allowing noninfringing circumvention of merged controls might cut more broadly than necessary to avoid interference with the congressional goal of allowing circumvention of rights controls for noninfringing purposes. This potential overbreadth might, however, simply be accepted. After all, the permitted activity is likely to be small in quantity, since only technologically skilled persons would be able to com-

---

129. Because of the language of the device bans, though, a device's usefulness for circumventing protection measures applied to works not protected by copyright law *is* relevant in determining whether the device is prohibited. *Id.* § 1201(a)(2), (b)(1) (defining prohibited technology by its uses for circumventing technology that "controls access to a work protected under this title" or that "protects a right of a copyright owner under this title in a work"). Thus, if a device has a commercially significant purpose of circumventing access measures that control access to works in the public domain, it would not be illegal under 17 U.S.C. § 1201(a)(2)(B). Its legality would still, however, depend on the purpose for which it was "primarily designed or produced," and on the way in which it is marketed. *Id.* § 1201(a)(2)(A), (C).

130. Ginsburg, *supra* note 26, at 16.

mit such circumventing acts. Moreover, such acts are unlikely actually to be penalized even under the current statute without a merged-control exemption, since such circumvention occurs in private. If, on the other hand, the permitted undesirable activity is significant enough to warrant imposing § 1201(a)(1)'s prohibition, the exemption could be more narrowly drawn. It might distinguish between different types of merged control measures, allowing noninfringing circumvention where the control is primarily operating as a rights control but not where it primarily operates as an access control. Or it might distinguish between types of circumventions, exempting only those designed to do something more than merely obtain unauthorized access to a work without payment.[131]

The forum in which the exemption is adopted could determine the precise scope of an exemption from the circumvention ban in the case of merged control measures. The most obvious forum is Congress, which could amend the statute to provide for the exemption. Another possible forum is a Copyright Office rulemaking. Section 1201(a)(1) directs the Librarian of Congress to hold a rulemaking proceeding every three years to determine whether the ban on access-control circumvention is likely to adversely affect users' ability to make noninfringing uses of any "particular class of copyrighted works."[132] If the Librarian makes such a determination, then the circumvention ban does not apply to users of a copyrighted work that is in the identified "particular class."[133] The statute thus gives the Librarian, on recommendation of the Register of Copyrights, the power to adopt temporary, partial exemptions to the circumvention ban (though not to either of the device bans).

The Librarian's first rulemaking proceeding under the statute was completed in October 2000, and briefly considered the possibility of an exemption with respect to merged control measures. The Register, however, concluded that, at the time of the rulemaking, the evidence did not establish that merged control measures posed a significant enough prob-

131. Commentators have suggested this type of approach for other applications of § 1201(a). *See, e.g.*, Ginsburg, *supra* note 26, at 16 ("[I]t may become necessary to modify the scope of the § 1201(a) access right, to continue to provide strong protection against unauthorized *initial* acquisition of a copy of a protected work, but to allow for circumvention in order to engage in fair uses, once the copy has been lawfully acquired."); Samuelson, *supra* note 2, at 539 ("Courts should distinguish between circumvention aimed at getting unauthorized access to a work and circumvention aimed at making noninfringing uses of a lawfully obtained copy. Section 1201(a)(1) is aimed at the former, not the latter.") (citations omitted).

132. 17 U.S.C. § 1201(a)(1)(C).

133. *Id.* § 1201(a)(1)(B), (D).

lem to require that the rulemaking address it.[134] Nonetheless, the Register noted that "[i]f in a subsequent rulemaking proceeding one could show that a particular 'copy' or 'use' control could not in fact be circumvented on a legitimately acquired copy without also circumventing the access measure, one might meet the required burden on this issue [of substantial or concrete harm to users].[135] The Copyright Office stated its intent to continue to monitor the issue and perhaps to consider it in connection with future exemption rulemakings.[136]

At least two features of the rulemaking proceeding, however, suggest that it is not a hospitable forum for providing relief to those who wish to circumvent a merged control measure in order to engage in noninfringing use. The first problem is that the statute empowers the Librarian to adopt an exemption from the circumvention ban if users are likely to be adversely affected in their ability to make noninfringing uses of any "particular class of works."[137] In the 2000 rulemaking, the Register, however, rejected any definition of a class of works "based on the status of the user or the nature of the use."[138] This may make it difficult to adopt an appropriate exemption for merged control measures. As discussed above, an appropriately tailored limitation on § 1201(a)(1) for merged controls would exempt from liability anyone who circumvents a merged control to make a noninfringing use of the work protected by the control. That exemption, however, would require defining the "particular class of works" to which the exemption applies by reference in part to the nature of the use to be made by the circumventing party—a definitional criterion expressly rejected by the Register of Copyrights in 2000 as beyond the statutory scope of the Librarian of Congress's rulemaking authority.[139]

---

134. Exemption to Prohibition on Circumvention of Copyright Protection Systems for Access Control Technologies, 65 Fed. Reg. 64,556, 64,568 (Oct. 27, 2000).

135. *Id.*

136. *See id*. The Copyright Office specifically stated:

> At present, on the current record, it would be imprudent to venture too far on this issue in the absence of congressional guidance. The issue of merged access and use measures may become a significant problem. The Copyright Office intends to monitor this issue during the next three years and hopes to have the benefit of a clearer record and guidance from Congress at the time of the next rulemaking proceeding.

Id.

137. 17 U.S.C. § 1201(a)(1)(B)-(D).

138. Exemption to Prohibition on Circumvention of Copyright Protection Systems for Access Control Technologies, 65 Fed. Reg. at 64,560.

139. The Register did recognize the permissibility for rulemaking purposes of classifying works *in part* "by reference to the medium on which the works are distributed or even to the access control measures applied to them." *Id*. Thus, for example, an exemp-

A second difficulty in solving the merged control problem through the triennial rulemaking is the high burden that proponents of an exemption must meet in order to persuade the Librarian to act. The 2000 rulemaking made clear that those proposing an exemption bear the burden of demonstrating that § 1201(a)(1)'s ban on circumvention "has a substantial adverse effect on noninfringing use," and that the decisionmaker will focus on whether there are "distinct, verifiable, and measurable impacts."[140] This standard could be difficult to meet with respect to the impact of merged control measures on noninfringing users. The Copyright Office has indicated that if an access control's adverse effect on noninfringing uses is "confined to a relatively small number of users," then the adverse effect does not rise to the "substantial" level required to adopt an exemption.[141] Because most circumvention devices seem likely to be prohibited even where people could use those devices to circumvent access or rights controls in order to make noninfringing uses, those adversely affected by treating a merged control measure as an access control are those who wish to circumvent the merged control in order to make noninfringing uses *and* who have the technological capability to do so.[142] That seems likely, in most cases, to be a relatively small number of people. The rulemaking proceeding may therefore view the adverse affect of protecting merged control measures as access controls as *de minimis* and not within the Librarian's power to address.

These problems suggest that the triennial rulemaking under § 1201(a)(1) may not be well suited to address concerns about the effect of merged control measures on noninfringing uses of copyrighted works. Indeed, the Register herself noted the rather constrained scope of the Librarian's rulemaking authority in the first rulemaking proceeding: "While many commenters and witnesses made eloquent policy arguments in support of exemptions for certain types of works or certain uses of works,

---

tion might be possible for musical works and sound recordings distributed on CD using a specific merged control system. But such an exemption would still be too broad, since it would exempt from liability for circumvention both those who, post-circumvention, engage in permitted uses and those who engage in outright infringement.

140. *Id.* at 64,558.

141. *Id.* at 64,569.

142. While the number of people directly adversely affected may be small, they may be a particularly important group for copyright purposes. Particularly where the person wishing to circumvent a merged control wants to do so in order to make a transformative fair use of the work, the benefit of the post-circumvention use may extend far beyond the user, to all of those who might encounter the transformative work. After all, creators and publishers of works of authorship may be a relatively small group of people as part of the nation's entire population, but we consider them particularly deserving of protection for their work because the rest of the population benefits substantially from their efforts.

such arguments in most cases are more appropriately directed to the legislator rather than the regulator who is operating under the constraints imposed by section 1201(a)(1)."[143] The need to address the problems posed by merged control measures may similarly be a concern better directed to Congress than to the Librarian.

C. Exempt Noninfringing Circumvention of Merged Control Measures as Part of Broader Limitation on Rights Against Circumvention

Another way to ensure that those who wish to circumvent a merged control measure for noninfringing purposes may do so would be to adopt more general limitations on the ban against circumventing access-control measures. As Jane Ginsburg has noted, copyright law traditionally did not grant copyright owners an exclusive right of access to their works once they are made publicly available, but § 1201 may effectively grant such a right. Professor Ginsburg further points out that because Chapter 12 does not protect an author's control over access as a § 106 exclusive right under copyright law, the copyright owner's control over access is not subject to the normal limitations imposed on copyright rights, including fair use. Instead, the copyright owner's control over access is subject only to the very limited exceptions listed in § 1201.[144] This clearly presents difficulties for copyright law's traditional role of balancing the interests of copyright owners and the public:

> [W]ithout an appropriate fair use limitation, the access right under § 1201 becomes much more than such a component [of copyright]. It becomes instead an Uber-copyright law, rigid as to specified exceptions, and therefore freed of further inquiry into the balance of copyright owner rights and user privileges that the fair use doctrine—and the general structure of copyright law—require.[145]

Professor Ginsburg therefore recommends subjecting copyright owners' legal right to prevent circumvention of access controls under § 1201 to additional exemptions that take into account the copyright system's

---

143. Exemption to Prohibition on Circumvention of Copyright Protection Systems for Access Control Technologies, 65 Fed. Reg. at 64,562.

144. *See* Ginsburg, *supra* note 26, at 11 ("[A]ccess controls may be a measure too crude to accommodate a variety of non infringing uses, including reproduction of unprotected information contained within a copyrighted work, and 'transformative' fair uses . . . .").

145. *Id*. at 17.

need to allow unauthorized access and use of copyrighted works in some instances.[146]

Indeed, Professor Ginsburg suggests that it might be necessary to modify § 1201 "to allow for circumvention in order to engage in fair uses," once a user has lawfully acquired a copy of the protected work.[147] The statute might, for example, provide that the act of circumvention is fair if a circumventor's post-circumvention use qualifies as fair use. Or the statute might direct a court in such an instance to weigh all of the circumstances surrounding the circumvention to determine whether to allow the circumvention, just as courts in copyright infringement cases weigh all of the circumstances surrounding a defendant's use of copyrighted material in order to determine whether the use is a fair use.

Such a general approach to limiting the copyright owner's legal control over access via technological protections could also easily accommodate the specific concerns relating to merged control measures.[148] Someone who circumvents a merged control measure in order to make a noninfringing use of the protected work engages in conduct that copyright law has chosen to privilege by excluding it from the copyright owner's exclusive rights. A general exemption from the ban on circumventing access controls where the circumvention merely allows the user to make entirely legal uses of the work would address the principal difficulty raised by copyright owners' use of merged control measures. Two current legislative proposals would provide such a general exemption.[149] Both would

146. *Id.* at 16 (noting that "some traditional defenses may remain appropriate, others may not, but new ones may be needed"); *see also* Thomas Heide, *Copyright in the E.U. and United States: What "Access Right"?*, 2001 EUR. INTELL. PROP. REV. 469, 475-77 ("From this perspective, it becomes necessary to apply appropriate safeguard measures so that rights and limitations to copyright remain unaffected and introduce appropriate limitations and exceptions to any access centered rights structure.").

147. Ginsburg, *supra* note 26, at 16.

148. On the other hand, if the kinds of limitations on access controls that Professor Ginsburg proposes were to be adopted by means of a set of more specific exemptions, then one of those exemptions could address the specific problem of merged controls.

149. *See* Digital Media Consumers' Rights Act of 2003, H.R. 107, 108th Cong. (2003); Digital Choice and Freedom Act of 2003, H.R. 1066, 108th Cong. (2003). The former bill would allow circumvention if it "does not result in an infringement of the copyright in the [protected] work," H.R. 107 § 5(b), while the latter would permit circumvention if "necessary to make a non-infringing use of the [protected] work" and if "the copyright owner fails to make publicly available the necessary means to make such non-infringing use without additional cost or burden" to the user, H.R. 1066 § 5. In addition, both bills would allow the manufacture and dissemination of circumvention devices for noninfringing purposes. *See* H.R. 107 § 5(b); H.R. 1066 § 5.

allow the circumvention of access and rights controls if the circumventing party did not commit copyright infringement.

V. CONCLUSION

Copyright owners who wish to use technological measures to protect their works no doubt consider many variables in choosing which controls to use. Many of those variables may have little or nothing to do with the law, but the nature and degree of legal protection available against circumvention of technological controls no doubt plays at least a part in the decision for many copyright owners. Copyright owners seeking the maximum legal protection possible for their control systems may adopt systems that merge an access-control mechanism and a rights-control mechanism into a single system because of the added protection such a choice would provide. But if such merged control measures enjoy all the protection of both access controls and rights controls, then Congress's objective in carefully treating the different types of control measures distinctly in order to provide breathing room for noninfringing uses of copyrighted works will be significantly undermined. Congress should therefore consider amending the anticircumvention provisions of the Copyright Act to deal specifically with merged control measures in a way that continues to protect copyright owners' rights and the public's ability to make noninfringing uses.

DRM AS AN ENABLER OF BUSINESS MODELS: ISPS AS DIGITAL RETAILERS

By Lionel S. Sobel†

TABLE OF CONTENTS

I. THE QUEST FOR BETTER BUSINESS MODELS

Better business models are the Holy Grail of the digital age. Even Alex Doonesbury has joined the quest.[1] Alex is the daughter of Mike Doonesbury in Garry Trudeau's syndicated comic strip, so her search can take as long as Trudeau likes. Things are more urgent for those in the real world, especially for those in the entertainment industry. Unauthorized digital

† Editor, Entertainment Law Reporter; Distinguished Scholar, Berkeley Center for Law & Technology; Lecturer, Boalt Hall School of Law, University of California, Berkeley.

1. Garry Trudeau, *Doonesbury*, SAN FRANCISCO CHRONICLE, Jan. 19, 2003, at Sunday Comics 1.

reproduction and distribution have shattered traditional music industry business models and are on the verge of doing the same to movie industry models. The question is what, specifically, can be done about it. This is a difficult question to answer.

Proof that the question is difficult (if proof be necessary) can be found in the pages of the nation's leading business periodical, *The Wall Street Journal*. In an editorial triggered by a U.S. Naval Academy investigation of midshipmen suspected of downloading MP3 files, *The Wall Street Journal* recently advised the record industry, quite unhelpfully, that it needs a new business model.[2] This particular editorial criticized the record industry as one "still wedded to an LP-era business model." It was also dismissive of "MusicNet" and "pressplay," the record industry's maiden tests of new models based on digital distribution.[3]

The Wall Street Journal did not, however, offer an alternative business model it would find praiseworthy. Therein lies the rub. It is one thing to say a new model is necessary. It is quite another to suggest how that model might work. A general description of how a new model may work is not enough, and *The Wall Street Journal* failed to provide even that. The devil is in the details.

Keeping in mind that seemingly attractive concepts are often undone by their necessary details, I nevertheless suggest a business model that has promise: Internet service providers (ISPs) should become digital retailers for digital works of all kinds—music, movies, television programs, photographs, books, periodicals, and software. Under this model, ISPs would license digital works from their copyright owners at wholesale prices set by the owners. ISPs would then sell the digital works to their subscribers at retail prices set by the ISPs.[4]

Many groups would benefit from this model. ISPs would embrace this model because of its potential for great profit. Consumers would embrace this model because it gives them the choice and convenience they crave despite making them pay for digital works. Moreover, digital middlemen—website operators, peer-to-peer (P2P) networks, newsgroup and chat room hosts, Internet search engines, and online radio and television stations—could serve as promoters and distributors without fear of direct, contributory, or vicarious copyright liability. Computer and consumer electronics manufacturers and software companies would be able to invent and innovate to the best of their abilities without regulation of their prod-

2. *Face the (Digital) Music*, WALL ST. J., Dec. 2, 2002, at A18, *available at* http://www.freerepublic.com/focus/news/799006/posts (last visited May 3, 2003).

3. *Id*.

4. *See infra* Part III.A (giving a more detailed description of this model).

ucts' designs. And although copyright owners would lose the right to prevent the unauthorized digital redistribution of their works, they would gain the ability to set their own wholesale prices in the form of royalties paid by ISPs.

Digital Rights Management technology (DRM) makes this business model possible. DRM encompasses a variety of technologies used to identify digitized works[5] and to control their use.[6] Although *The Wall Street Journal* did not offer the record industry any suggestions for a new business model, others have offered suggestions. All of these suggested business models exhibit some DRM features.[7] Thus, DRM appears to be at the foundation of whatever business models will actually succeed in the digital age. Part II begins by describing a variety of these DRM-based business models. Some are being used already.[8] Others have been proposed but are not yet being used.[9] These models employ several different DRM technologies imposing a wide range of controls, from none to extensive, over the design of equipment used by consumers and the ways in which consumers may use the works they acquire. In a table, I place these models along this spectrum of control so that their relationship to each other can be seen.[10] I then describe the "ISPs as Digital Retailers" model and place it along the spectrum of control so it too can be seen in relation to others.[11] Following this, I specifically compare the Digital Retailers model to the "Tax and Royalty System," another promising and practical model that has attracted some attention and support.[12] I conclude that the Digital Retailers model satisfies more objectives than the Tax and Royalty System.[13] Finally, I acknowledge that the Digital Retailers model is not problem-free and identify several problems that would need to be solved in order for the Digital Retailers model to be successful.[14]

---

5. See, e.g., 17 U.S.C. § 1202(c) (2000) (defining "copyright management information"); WIPO Copyright Treaty, Dec. 20, 1996, art. 12(2) (defining "rights management information"), *available at* http://www.wipo.int/clea/docs/en/wo/wo033en.htm.

6. *See, e.g.*, 17 U.S.C. § 1201(a)(3)(B) (2000) (defining technical measures that "effectively control[] access to a work"); 17 U.S.C. § 1201(b) (2000) (prohibiting in most cases technology that circumvents access controls on a copyrighted work); WIPO Copyright Treaty, *supra* note 5 (defining "rights management information").

7. *See infra* Part II.D.

8. *See infra* Parts II.C and II.D.2.

9. *See infra* Parts II.B and II.D.1.

10. *See infra* Part II.D.2.

11. *See infra* Parts III.A and III.B.

12. *See infra* Part III.B.

13. *See infra* Part III.C.

14. *See infra* Part III.D.

II. DRM-BASED BUSINESS MODELS

A. The Role of Control

DRM's ability to give copyright owners the ability to control the use of their works is both the beauty of DRM (from the point of view of copyright owners) and its bane (from the point of view of many consumers and technology companies). As a result, it is useful to begin with a few words about the role of control by copyright owners and technology companies.

Copyright owners value control over their works because unauthorized copying and redistribution destroys their ability to market their works in two ways. First, the copyright industry's business models envision selling multiple copies of a work at per copy prices that are a fraction of the cost of producing those works. Uncontrolled copying and redistribution destroys this plan because unauthorized digital copies displace sales and performances. Second, unauthorized copying and redistribution of copyrighted works prevents copyright owners from changing the price of their works over time in ways they hope will maximize their incomes.

The marketing section of every thorough business plan depends on pricing strategies. Ideally, copyright owners should charge higher prices to those customers who value the sellers' goods and are best able to afford higher prices. Similarly, owners should charge lower prices to customers who do not value their goods as much or are less able to afford them. Economists refer to this as "price discrimination." A successful business model should not force copyright owners to charge the same price to all buyers because the owners will lose the ability to maximize profits through price discrimination.[15]

Some have argued that copyright owners do not have the ability to engage in perfect price discrimination.[16] But successful business plans do not require perfect price discrimination. Copyright owners only need the ability to price discriminate a little, as in these familiar examples:

- Hardcover books come out before and cost more than paperback reprints.
- Most movies come out in theaters before they are available to rent on DVDs and videocassettes. Movie theater tickets cost more than rentals; rentals cost more than viewing movies on pay-TV; and viewing movies

15. *See, e.g.*, ProCD v. Zeidenberg, 86 F.3d 1447, 1449-50 (7th Cir. 1996) (explaining price discrimination).

16. Neil Weinstock Netanel, Impose a Noncommercial Use Levy to Allow Free P2P File-Swapping and Remixing 19-20 (Nov. 2002) (unpublished manuscript, *available at* http://www.utexas.edu/law/faculty/nnetanel/Levies_chapter.pdf).

on pay-TV generally costs more than watching movies on advertiser-supported TV.

- Buying a DVD or videocassette costs more than renting one.
- New albums by musical artists cost more than "greatest hits" compilations; these compilations cost more than multi-artist albums compiled by theme.
- Full-featured versions of computer software cost more than "lite" versions; and "lite" versions cost more than "trial" versions.

In other words, business plans for the marketing of copyrighted works are based on the ability to do sequential but separate releases of those works. In entertainment businesses, the sequence of releases for successful works spans a long time. Copyright owners seek control over the use of their works because uncontrolled copying and redistribution of works interferes with the success of long-term sequential release.

Technology companies have similar concerns, but not to the same degree, because for them design innovations are central to their business plans. They fear that legal regulation of their products' features would interfere with product innovation, and thus interfere with their business plans. For example:

- Computers running text-only DOS operating systems were perfectly adequate for word processing and spreadsheets. If legal regulation had prohibited the implementation of graphical user interfaces on the grounds that such interfaces could be used to infringe photograph copyrights or display pornography, the computer and software industries may have been frozen at their pre-Windows and pre-Macintosh stages of development.
- Personal computers were widely used in business and by consumers before PCs could be used to access the Internet. If legal regulation had prohibited the use of telephone modems on the grounds that modems can be used to infringe copyrights or transmit pornography, email would not be available today to businesses or consumers.

Therefore, the basic tension between the copyright and technology industries is the tension between the degree of control copyright owners would like to have over their works and the extent to which technology companies should legally be required to facilitate and respect that control. Because control is so central to the significance of DRM, this article next describes several digital business models that exhibit a different degree of control over a phenomenal range. On one end of this spectrum, the "anti-

copyright"[17] models advocate almost no control over the distribution of copyrighted works. On the other extreme, the "beyond-copyright"[18] models give owners even more control over copying and distribution than granted by copyright protection. The "copyright-based"[19] models occupy the middle of this spectrum of control.

B. The "Anticopyright" Model

The anticopyright model would eliminate copyright entirely in the online digital domain.[20] DRM may play a role in this model, but only to identify authors whom audiences may choose to compensate with "tips."[21] No one seems to have suggested that eliminating copyright and replacing it with tips would actually succeed in providing a living wage for anyone, and the current online tip-systems have so far given musicians only modest compensation.[22]

C. The "Beyond-Copyright" Models

At the other extreme from the anticopyright model are two models that would provide even more protection than current copyright laws.

The first beyond-copyright model allows publishers to use DRM to control access to works, even those in the public domain, to prevent their unauthorized copying and distribution. Although I could find no commentary on this first model, the technology needed for the model seems to exist. Passwords would control access to works, and encryption and watermarks[23] would prevent unauthorized uses. Under this model, circumvention would be a punishable offense, but everyone would be free to digitize and distribute their own versions of works in the public domain, at their own expense, without liability. This model, however, would prevent anyone other than the publisher from copying existing digital versions. In other words, the model would prevent users from free riding on a pub-

17. *See infra* Part II.B.

18. *See infra* Part II.C.

19. *See infra* Part II.D.

20. *See, e.g.*, Mark S. Nadel, Questioning the Economic Justification for Copyright 3 (Feb. 21, 2003) (unpublished manuscript, *available at* http://papers.ssrn.com/sol3/papers.cfm?abstract_id=322120); Netanel, *supra* note 16, at 17.

21. *See, e.g.*, TipJar LLC, *Internet Treasury Home Page* (website allowing online tipping of recording artists), *at* www.tipjar.com (last visited Mar. 20, 2003); Musiclink, *Give It. Get It. Not For Profit* (same), *at* www.fairtunes.com (last visited Mar. 20, 2003).

22. *See, e.g.*, Chris Kelsey, *Bandwidth: Passing the Virtual Hat*, Onstage (Dec. 1, 2001), *at* http://onstagemag.com/ar/performance_bandwidth_passing_virtual (quoting a band member saying that "Nobody every contributed" a tip through the voluntary payment systems until "someone gave us a contribution through Fairtunes . . . [of] $300!").

23. *See infra* Part III.A.2 (describing watermark technology).

lisher's investment in digitizing a work—even a work in the public domain.

The second beyond-copyright business model does not go quite as far. Companies practicing this model would use DRM to control access to public domain materials, but would not control copying or redistribution of these works. For example, Westlaw and LEXIS distribute digital versions of public domain works to subscribers, unencrypted, with copying and redistribution controlled, if at all, merely by contract. The United States government also uses this model in its pay-per-page PACER system for the digital distribution of federal court judicial decisions.[24]

D. Copyright-Based Models

Between the anticopyright and beyond-copyright models are two sets of copyright-based models. Both sets of models seek to extend existing copyright law into the digital domain. One set would impose statutory licenses that authorize digital uses of copyrighted works. The other set would give copyright owners discretion over licensing terms and control over unauthorized uses of their works.

1. Statutory License Models

Two statutory license models have been proposed, one by Neil Netanel[25] and the other by William (Terry) Fisher.[26] Because both would require amendments to the Copyright Act, neither has yet been put into practice.

Professor Netanel has proposed a "Noncommercial Use Levy."[27] This model permits noncommercial copying, distribution, performance, and adaptation of copyrighted works in return for levies paid by the providers of products and services whose value is enhanced by file swapping.[28] A statutory license would allocate these collected levies among the categories of copyright owners (record companies, movie producers, book publishers, and so forth), and then among individual copyright owners within

24. PACER Service Center, *Public Access to Court Electronic Records: Overview*, *at* http://pacer.psc.uscourts.gov/pacerdesc.html (last visited Mar. 14, 2003).

25. Netanel, *supra* note 16.

26. William Fisher, Digital Music: Problems and Possibilities (Oct. 10, 2000) (unpublished manuscript, *available at* http://www.law.harvard.edu/Academic_Affairs/coursepages/tfisher/Music.html); *see also Fisher @ FMC: Replace Copyright with Watermarks, Taxes*, *available at* http://www.corante.com/copyfight/20030101.shtml#17322 (Jan. 8, 2003).

27. Netanel, *supra* note 16.

28. *Id*. at 28-38.

each category.[29] Those entitled to levies would receive them in proportion to how often their works were used.[30] Unless affected industry segments themselves agreed on the levies, Copyright Office arbitrations would determine the levy amount applied to each type of product or service.[31] Presumably, Copyright Office arbitrations would also settle disputes over allocation to copyright owners.

Professor Fisher has proposed a "Tax and Royalty System."[32] Under this system, the government would tax ISP access and any technology used to perform music, including MP3 players, hard drives, and computers. The collected revenues would be distributed to copyright owners in proportion to how often their works are accessed. Professor Fisher's proposal focuses on the recorded music industry in particular, but there is no reason his Tax and Royalty System could not be used to compensate copyright owners in other industries as well.

The Noncommercial Use Levy and the Tax and Royalty System both use DRM to monitor the frequency with which users access particular copyrighted works.[33] Under both models, ISPs monitor the flow of copyrighted files through their routers and record the frequency with which a copyrighted work appears. The compiled data is used to allocate collections proportionately among copyright owners.

Royalty setting and royalty allocation, the two key features of these models, are based on well-established elements of existing copyright law. Copyright Office arbitrations already set statutory license fees and allocate collected fees in connection with cable and satellite retransmissions of copyrighted movies, television programs, the musical compositions in their soundtracks,[34] and with consumer duplication of digital music recordings.[35] The same arbitrations also determine the license fees for certain online digital performances of music recordings[36] although Congress

29. *Id*. at 38-39.

30. *Id*. at 39.

31. *See* 17 U.S.C. §§ 801-803 (West 1996 & Supp. 2002).

32. Fisher, *supra* note 26.

33. *See infra* Part III.A.2 (describing watermarking and fingerprinting technologies that can monitor the frequency with which individual works are used).

34. 17 U.S.C. § 111(d) (2000) (describing statutory license fees and allocation for secondary transmission of copyrighted works by cable companies); 17 U.S.C. § 119(b) (2000) (describing statutory license fees and allocation for secondary transmission of television stations by satellite carriers); 17 U.S.C. § 122 (2000) (describing statutory license fees and allocation for secondary transmission of television broadcasts by satellite carriers within local markets).

35. 17 U.S.C. §§ 1003-1008 (2000).

36. 17 U.S.C. § 114 (2000).

itself has already specified the allocation of digital performance royalties among those entitled to receive them.[37]

Although the Noncommercial Use Levy and the Tax and Royalty System are similar, they differ in at least one important respect. The Noncommercial Use Levy permits users to create new versions of digital works in addition to making and redistributing copies.[38] The Tax and Royalty System, on the other hand, does not contemplate the creation of new versions; it simply authorizes copying and redistribution.[39] Thus, the Tax and Royalty System leaves more control in the hands of copyright owners, namely the right to license the creation of new versions of their works on terms agreed to in private negotiations.

2. Models Giving Copyright Owners Discretion and Control

Several other models give copyright owners discretion over licensing terms and control over unauthorized uses of their works rather than impose statutory licenses. These models are being used now (and what follows are my own descriptions of their key features).

One model gives copyright owners access control, using passwords as the only DRM feature. This model does not control copying or redistribution, and thus does not require encrypting the distributed content. Familiar examples of this model include the online editions of *The New York Times* and *The Wall Street Journal*. Both websites require registration to obtain a password that is necessary for access. Use of *The New York Times*' site is free to anyone. By contrast, *The Wall Street Journal*'s site requires all users, including those who subscribe to the paper edition, to pay an on-line subscription fee. Both companies enforce their password requirements using technologies that run on their own servers. A user's computer does not require password-related design features or website-specific software.

A second model gives copyright owners copy and redistribution control in addition to access control. Under this model, encryption restricts access to those using special software provided by or on behalf of copyright owners. This software controls what those who are given access may do with materials, allowing only authorized uses. Familiar examples of this model include publications in the Adobe eBook format, and audio and video materials in the RealMedia and Windows Media formats.

A third model gives copyright owners control over access, but not over copying or redistribution, by using encryption instead of password protection. This model requires authorized users to have specially designed

37. *Id.* § 114(g)(2).
38. Netanel, *supra* note 16, at 29.
39. *See* Fisher, *supra* note 26.

equipment to receive and decrypt materials. Companies that manufacture the necessary equipment voluntarily incorporate the necessary design features into their equipment; they are not compelled to do so by law. This model is used by cable systems and satellite TV companies.

A fourth model uses encryption to give copyright owners control over access, copying, and redistribution. This model, like the previous model, requires authorized users to have specially designed equipment to access and decrypt materials. Manufacturers of this equipment also incorporate necessary design features voluntarily; they are not required by law to do so. This model is used in connection with movie DVDs which are encrypted and then decrypted using the Content Scramble System (CSS).[40] The record industry's Secure Digital Music Initiative (SDMI) would have used this model.[41] Although SDMI was not implemented in connection with commercially released CDs, some record companies are now using similar technologies based on this model.[42]

Finally, a fifth model uses DRM to give copyright owners access, copy, and redistribution controls over digital works that are not encrypted, but contain digital data that prevent unauthorized uses of those works. Because these works are not encrypted, this model works only if computers and consumer electronics devices contain circuitry that recognizes and responds to the authorized use information. Without such circuitry, computers and other devices would play unencrypted works and permit them to be copied and redistributed. One example of this model is the Serial Copy Management System, intended to permit record companies to control digital copying of recorded music.[43] This system, which is at the heart of the Audio Home Recording Act of 1992, requires digital audio recorders to be equipped with circuitry that prevents them from being used to make serial copies (that is, copies of copies) of digital recordings.[44] The commercial significance of that ban was largely undercut by the advent of MP3 technology for storing recorded music and consumers' use of computers, rather than digital audio recorders, to copy and redistribute MP3

40. *See* Universal City Studios v. Corley, 273 F.3d 429, 436-37 (2d Cir. 2001); Dean S. Marks & Bruce H. Turnbull, *Technical Protection Measures: The Intersection of Technology, Law and Commercial Licenses*, 46 J. COPYRIGHT SOC'Y U.S. 563, 578-86 (1999).

41. Marks & Turnbull, *supra* note 40, at 592-95.

42. *See, e.g.*, Fat Chuck's, *Corrupt CDs + News*, *at* http://www.fatchucks.com/z3.cd.html (updated Nov. 9, 2002).

43. *See* Recording Indus. Ass'n, Inc. v. Diamond Multimedia Sys., Inc., 29 F. Supp. 2d 624, 631-32 (C.D.Cal. 1998), *aff'd*, 180 F.3d 1072 (9th Cir. 1999); Marks & Turnbull, *supra* note 40, at 592-95.

44. 17 U.S.C. § 1002 (2000).

files. MP3 technology undermines the Serial Copy Management System because the Audio Home Recording Act exempts computers from the need to have anti-copying circuitry.[45]

Nevertheless, this fifth model remains at the forefront of current debates about the proposed "Broadcast Flag System" for restricting the use of unencrypted digital television broadcasts.[46] These debates are the result of an FCC mandate that digital television broadcasting be introduced nationwide by 2006.[47] Movie and television producers are not going to provide expensive content for digital TV broadcasts if that content can easily be copied and forwarded over the Internet to recipients around the world. As a result, the lack of effective copy protection methods may hinder the development of digital TV broadcasting by greatly reducing the amount of attractive programming that is made available for it.

The Broadcast Flag copy protection method was the centerpiece of a bill in the 107th Congress formally entitled the "Consumer Broadband and Digital Television Promotion Bill."[48] The bill, commonly referred to as the "Hollings Bill," would have required "digital media devices" to provide "effective security for copyrighted works."[49] The 107th Congress adjourned without enacting or even voting on the Hollings Bill, but that does not delay the effective date of nationwide digital TV broadcasting.

With these developments in mind, the FCC recently issued a Notice of Proposed Rulemaking by which the Commission invited comments on whether it should adopt rules that would mandate the incorporation of copy protection technology into television receivers and other consumer electronics devices, such as digital TV recorders.[50] An alliance of copyright owners, broadcasters, and entertainment industry unions has urged the FCC to adopt a rule that would require devices to recognize and respond to "Broadcast Flags" included in digital TV broadcasts. These

45. 17 U.S.C. § 1001(5)(B)(ii) (2000); *Recording Indus. Ass'n, Inc.*, 29 F. Supp. at 631.

46. *Digital Broadcast Copy Protection*, MB Docket No. 02-230, FCC 02-231, at 2-3 (released Aug. 8, 2002) (Notice of Proposed Rulemaking), *available at* http://hraunfoss.fcc.gov/edocs_public/attachmatch/FCC-02-231A1.pdf (last visited May 5, 2003)..

47. *Advanced Television Systems and Their Impact upon the Existing Television Broadcast Service*, MM Docket No. 87-268, FCC 97-116, at 43 (released Apr. 21, 1997) (DTV Fifth Report and Order), *available at* http://www.fcc.gov/Bureaus/Mass_Media/Orders/1997/fcc97116.pdf (last visited May 5, 2003).

48. S. 2048, 107th Cong. (2002), *available at* http://thomas.loc.gov/cgi-bin/query/z?c107:S.2048: (last visited May 4, 2003).

49. *Id.* § 3(d).

50. *Digital Broadcast Copy Protection*, MB Docket No. 02-230, FCC 02-231 (released Aug. 8, 2002) (Notice of Proposed Rulemaking), *available at* http://hraunfoss.fcc.gov/edocs_public/attachmatch/FCC-02-231A1.pdf.

Broadcast Flags would indicate whether those broadcasts may be redistributed outside the recipient's home.[51] Broadcast Flags do not encrypt unencrypted digital TV signals. Therefore, the Broadcast Flag System would require devices that receive and process digital broadcasts to recognize whether particular signals may be redistributed outside the recipient's home. Additionally, those devices would not permit redistribution if a signal's Broadcast Flag does not authorize it.

The following chart recaps these business models (excluding the anti-copyright and beyond-copyright extremes). Those that protect copyright the most are at the top of the chart; those that protect copyright the least are at the bottom. The chart also reflects the technology required to implement each business model. Not coincidently, the chart shows that providing more control over copyrighted works requires more control over technology under the business models discussed thus far.

51. *Digital Broadcast Copy Protection*, MB Docket No. 02-230 (released Dec. 6, 2002) (Joint Comments of the Motion Picture Association of America, et al.), *available at* http://www.mpaa.org/Press/MPAA_Comments_02-230.pdf (last visited May 5, 2003).

Copyright Control	Business Model	Enabling Technology	Controls			Control over Technology
			Access	Copy	Redistrib.	
More ↕ Less	SCMS for digital audio music recorders; Broadcast Flag System for digital TV broadcasts	Watermarks: Equipment must contain legally mandated features	Yes	Yes	Yes	More ↕ Less
	CSS for DVDs; SDMI for music CDs	Encryption: Equipment must contain voluntarily installed features	Yes	Yes	Yes	
	Adobe eBook, RealMedia, Windows Media	Encryption: Requires only special software to read	Yes	Yes	Yes	
	Cable and satellite TV	Encryption: Equipment must contain voluntarily installed features	Yes	No	No	
	N.Y. Times/ Wall St. J. online	Passwords: No special user technology required	Yes	No	No	
	Tax and Royalty System	Watermarks: No special user technology required; watermarks used for royalty allocation only	No	No	No	
	Noncommercial Use Levy	Watermarks: No special user technology required; watermarks used for royalty allocation only	No	No	No	

III. ISPS AS DIGITAL RETAILERS MODEL

The birth of my Digital Retailers model occurred in connection with a panel discussion on P2P computing sponsored by the Berkeley Center for Law & Technology during the 2002 Spring semester. The discussion included a debate between panelists who advocated unimpeded P2P computing even when P2P networks were used for unauthorized distribution of digital files of copyrighted works and panelists who advocated imposing liability on facilitators of P2P computing if they knew their technologies were being used for unauthorized distribution of copyrighted works. The debate took place in the wake of *A&M Records, Inc. v. Napster, Inc.*[52] and much of the discussion dealt with the nuances of vicarious and contributory infringement, and with "safe harbors" under the Digital Millennium Copyright Act.[53]

The panel's organizers asked me to talk about whether there was a "solution" to the "P2P problem." It occurred to me that since P2P computing takes place on the Internet and all P2P users use ISPs to get access to the Internet, ISPs could play an important role in a possible solution. But I did not think that ISPs could solve the P2P problem at their own, unreimbursed expense. If ISPs are going to be used as *de facto* distributors of copyrighted digital works, ISPs could be made legal distributors of these works as well. ISPs could be persuaded to take on the role of authorized distributors by giving them financial incentives. In the world of physical goods, a retailer's financial incentive is the spread between the wholesale and retail prices of those goods. It seemed to me that the same incentive could be given to ISPs in return for their serving as digital retailers.

A. How the Digital Retailers Model Would Work

1. Overview

Under the Digital Retailers model, people would use the Internet much as they do now. They would connect to the Internet through dial-up or broadband accounts with ISPs. While online, they would visit websites, newsgroups, chatrooms, email servers, and P2P peers. And while visiting these destinations, they would download or stream digital content to their computers. But for digital content containing copyrighted works, the owners of the copyrights would have the right to digitally identify each work, its owner, and the wholesale royalty price to be paid by ISPs for its transmission to users.[54] As content identified in that fashion passed through

52. 284 F.3d 1091 (9th Cir. 2002).
53. 17 U.S.C. § 512(d) (2000).
54. *See infra* Part III.A.2 (describing the technology by which this can be done).

ISPs' routers to their users, ISPs would log those transmissions and bill users' accounts monthly for the content they received, at retail royalty rates set by ISPs, using the same billing methods by which ISPs now charge users for Internet access.

To protect users from downloading unwanted works[55] or incurring exorbitant charges, ISPs could send pop-up notices before the actual files are transmitted. These pop-up notices would inform users that files requiring payments are about to be sent and would display the cost of sending the file. These pop-up notices could look and work like virus warnings seen today, and users would respond to them by clicking "Yes" or "No" buttons.

2. Enabling DRM Technologies

For ISPs to become digital retailers, they must be able to track each user's access to digital versions of copyrighted works and record those users who download and purchase these digital versions. ISPs can monitor copyrighted file access using two types of existing DRM technologies: "watermarking" and "fingerprinting."

Digital watermarks are digital identifications inserted into digital copies of works when they are manufactured.[56] People cannot hear or see watermarks, but computers and software can detect them.[57] Few digital versions of works on the Internet contain watermarks because many digital copies of copyrighted works are created without watermarks. For example, when consumers digitally copy analog works from music cassettes, video tapes, photographs, and texts, they do not insert watermarks into the copies they make. Consumers can also strip a watermark off a digital work by converting the work to analog and then recording the work back into a digital format.

In addition to watermarking, copyright owners can create digital identifiers for copies of their works by "fingerprinting" a digital version of their work. Fingerprinting converts the work's content into a unique digital identification mark by applying an algorithm to selected features of that content.[58]

---

55. *See infra* Part III.D.2.

56. *See generally* Digimarc Corp., *Digital Watermarking Frequently Asked Questions*, *at* http://www.digimarc.com/products/support/faqs.asp (defining and discussing digital watermarking).

57. *Id.*

58. *See generally* Audible Magic Corp., *Home Page*, *at* www.audiblemagic.com (describing one patented audio fingerprinting process).

Together, watermarking and fingerprinting can provide digital identifications for every digital work that copyright owners choose to have identified. ISPs can use these identifications to recognize works transmitted as digital files through networks connected to ISPs, which includes transmissions from websites, over P2P networks, and as attachments to emails or instant messages. Information about the copyright owner of each watermarked and fingerprinted work could be stored in a database along with the wholesale royalty price the copyright owner has decided to charge for the work's transmission to the ISP's customer. As these works pass through ISPs' routers, ISPs would identify the works and determine their wholesale royalties by checking their watermarks or fingerprints against the database. ISPs would then apply their retail markup and charge their customers' accounts for works they download.

3. Implementation of the Technology by ISPs

Under the Digital Retailer model, the technology used to identify watermarked and fingerprinted files would reside on *ISPs' computers*, not on the end-users' computers or on consumer electronic devices. This distinction is important for four reasons.

First, putting the technology on ISPs' computers frees computer and consumer electronics manufacturers and software companies to innovate without legal restrictions on their products' designs. Although ISPs would have to acquire, install, and use the enabling technology just described, that technology would not have to be used by consumers or by operators of websites, P2P networks, newsgroups, and chatrooms.[59]

Second, putting the technology on ISPs' computers makes circumvention less likely. CSS, Adobe eBook and SDMI—all of which are implemented on consumers' computers—were circumvented quite quickly.[60] One recent technical report persuasively argued both that watermark detection technology implemented in software on users' computers or electronic devices could be easily defeated and that detection technology implemented in hardware makes the computers and devices obsolete too quickly.[61]

---

59. *See supra* Part III.A.2.

60. *See, e.g.*, Universal City Studios v. Corley, 273 F.3d 429, 436-37 (2d Cir. 2001); United States v. Elcom Ltd., 203 F. Supp. 2d 1111 (N.D.Cal. 2002); Scott A. Carver et al., *Reading Between the Lines: Lessons from the SDMI Challenge*, *available at* http://www.usenix.org/events/sec01/craver.pdf (visited Mar. 14, 2003).

61. Peter Biddle, et al., *The Darknet and the Future of Content Distribution*, *available at* http://crypto.stanford.edu/DRM2002/darknet5.doc (visited Mar. 14, 2003).

Third, all users of an online service connect to the Internet through ISPs, and thus can be billed by their ISPs for whatever copyrighted works they access. ISPs can already meter the bandwidth usage of each of their subscribers, and several ISPs may begin charging subscribers based on usage rather than flat monthly fees.[62]

Fourth, an Internet user could download many copyrighted works during a single online session. Furthermore, the royalties requested for these works could vary from fractions of a cent to hundreds of dollars. This presents both a problem and a potential solution.[63] Many website operators will likely use only royalty-free works to avoid driving away users unwilling to pay for copyrighted content.[64] To minimize the royalty and billing data that has to be processed, ISPs may create two channels for Internet access. One would allow access to royalty-bearing works; the other would not. The no-royalty channel would display icons to indicate that royalty-bearing works were available but blocked. Users would be able to switch back and forth between the two channels with a mouse click to selectively access royalty-bearing works or to avoid them.

4. Statutory License

The Digital Retailer model would require copyright owners, by statute, to permit the copying and redistribution of their works, but would not require copyright owners to watermark or fingerprint their works. By choosing not to watermark or fingerprint their works, owners would allow ISPs and subscribers to freely transfer the works. In contrast, the statute would require ISPs to pay royalty charges for each watermarked or fingerprinted copyrighted work downloaded. This arrangement is thus equivalent to a statutory license because it authorizes copying and redistribution of copyrighted works without negotiated licenses from copyright owners. But while this proposed license authorizes the use of copyrighted works, it also requires ISPs to pay royalties at whatever rates copyright owners set.

All ISPs that have relationships with end users who access copyrighted works would have to pay royalties. These ISPs would include:

- ISPs that provide Internet access to dial-up and broadband subscribers,

62. John Borland, *ISP download caps to slow swapping?*, CNET News.com (Nov. 26, 2002), *at* http://business2-cnet.com.com/2100-1023-975320.html.

63. *See infra* Part III.D (acknowledging and discussing other potential problems with the Digital Retailer model).

64. *See infra* Part III.A.4 (discussing copyright owners' royalty options, including the option not to charge a royalty).

- colleges and corporations that provide Internet access to students and employees,
- libraries that provide Internet access to patrons, and
- coffee shops, airports and other public places that provide Wi-Fi access to customers and travelers.

Currently, most colleges, corporations, libraries, and Wi-Fi-equipped coffee shops do not have billing relationships with their users.[65] These providers have two options: (1) create billing relationships with their users or (2) allow users to access only the no-royalty channel described above.[66]

ISPs themselves would not have to bear the cost of copyright royalties. Instead, they would be authorized to charge subscribers for the water-marked and fingerprinted files they receive, presumably at a rate greater than the copyright owner's fee. In most cases, a markup of 100% is likely. That is, ISPs would retain about 50% of the *retail* price paid by subscribers, and would pay about 50% to copyright owners. This is the traditional split between retailers and publishers in the book business, between retailers and record companies in the music business, and between theater owners and distributors in the movie business.

But a 100% markup from wholesale or a 50/50 split of retail would not be required. In the world of physical goods, retailers are as varied as Rodeo Drive boutiques whose markups may exceed 100% to Main Street warehouse-style discount stores whose markups may be 20% or less. In the world of digital content, ISPs may use low retail prices as a competitive tool to attract subscribers from ISPs that charge higher prices. Some ISPs may offer subscribers bulk-purchase plans, just as cell phone companies offer local and long-distance packages as alternatives to minute-by-minute charges.

B. The Digital Retailer Model Compared to Other Business Models

If the Digital Retailer model were placed in the business model chart, it would be slotted above the Tax and Royalty System, but beneath the others:

---

65. But some Wi-Fi-equipped airports will have a billing relationship with its users. *See* Reuters, *AT&T Wireless to Provide Wi-Fi in Hotels, Airports* (Jan. 28, 2003), *available at* http://www.azcentral.com/shopping/0128NET-TELECOMS-ATT-REPORT-DC.html.

66. *See supra* Part III.A.3.

Copyright Control	Business Model	Enabling Technology	Controls			Control over Technology
			Access	Copy	Redistrib.	
More ↕ Less	SCMS; Broadcast Flag System	Watermarks: Equipment must contain legally mandated features	Yes	Yes	Yes	More ↕ Less
	CSS; SDMI	Encryption: Equipment must contain voluntarily installed features	Yes	Yes	Yes	
	Adobe eBook, RealMedia, Windows Media	Encryption: Requires only special software to read	Yes	Yes	Yes	
	Cable and satellite TV	Encryption: Equipment must contain voluntarily installed features	Yes	No	No	
	N.Y. Times/ Wall St. J. online	Passwords: No special user technology	Yes	No	No	
	ISPs as Digital Retailers	Watermarks and Fingerprints: Requires monitoring technology on ISPs' computers; watermarks and fingerprints used for royalty assessment and payment	No	No	No	
	Tax and Royalty System	Watermarks: No special user technology; watermarks used for royalty allocation only	No	No	No	
	Noncommercial Use Levy	Watermarks: No special user technology; watermarks used for royalty allocation only	No	No	No	

The Digital Retailer model is similar to the Tax and Royalty System because both rely on ISPs to collect royalties from their subscribers, both use DRM to identify digital works accessed over the Internet, and both use DRM-enabled identifications to allocate collections among copyright owners entitled to receive royalties. In addition, because the Digital Retailer model does not require access, copy, or redistribution controls, it allows technology companies to innovate with new product designs as under the Tax and Royalty System.

The Digital Retailer model, however, is preferable to the Tax and Royalty System. The Tax and Royalty System deprives copyright owners of the ability to determine the royalty value of their own works and to vary their prices over time. By contrast, the Digital Retailer model allows copyright owners to do both. The ability to vary prices over time—quite likely by reducing the royalties set for individual works as those works get older—is the way in which copyright owners will be able to price discriminate,[67] even with uncontrolled copying and redistribution.

The Tax and Royalty System also requires expensive and time-consuming legal proceedings, both to establish royalty rates and to distribute collected royalties.[68] For the Copyright Office to determine the statutory license fee for digital transmission of recorded music has required many steps: an arbitration, a decision by the Librarian of Congress, a Copyright Act amendment, a privately-negotiated interim agreement, and a still-pending judicial appeal.[69] One Copyright Office arbitration costing more than $41,000 was necessary to resolve conflicting claims to digital audio recording royalties totaling just $6.10 split between two songwriters and a music publisher.[70] Moreover, each of these proceedings involved works of just one type: recorded music in the digital transmission proceeding and musical compositions in the digital audio recording proceeding. Under the Tax and Royalty System, rate setting and royalty distribution

67. *See supra* Part II.A.

68. *See, e.g.*, Karen Fessler, Comment, *Webcasting Royalty Rates*, 18 BERKELEY TECH. L.J. 399 (2003) (describing the shortcomings of the CARP process).

69. *Rate Setting for Digital Performance Right in Sound Recordings and Ephemeral Recordings*, Docket No. 2000-9, Library of Congress: Copyright Office (Feb. 20, 2002), *available at* http://www.copyright.gov/fedreg/2002/67fr4472.html; *Determination of Reasonable Rates and Terms for the Digital Performance of Sound Recordings and Ephemeral Recordings; Final Rule*, Library of Congress: Copyright Office, 67 C.F.R. 130 (July 8, 2002), *available at* www.copyright.gov/carp/webcast_regs.html; Small Webcaster Settlement Act of 2002, H.R. 5469 (2002), *available at* www.copyright.gov/legislation; *Rates and Terms Available to Certain Small Commercial Webcasters* (Dec. 13, 2002), *available at* http://www.soundexchange.com/Rates_Terms.pdf.

70. *Digital Audio Recording Royalty Proceeding was Much Ado About Very Little . . . Measured in Dollars*, 23 NO. 1 ENT. L. REP. 7 (2001).

proceedings will be infinitely more complex than in those proceedings because digital works range from $600 computer programs to $1 recorded music tracks. Leaving software out of the plan altogether does not solve the problem: unlicensed MP3 files have been the most newsworthy, but the problem encompasses unlicensed redistribution of computer programs as well.

However, I acknowledge that tracking copyrighted works would be less cumbersome under the Tax and Royalty System than under the Digital Retailer model. The Tax and Royalty System does not require ISPs to determine or track which users have accessed particular works. This system may be able to allocate collections using data obtained by digital file sampling in much the same way that ASCAP and BMI sample radio play of musical compositions before allocating public performance royalties. The Digital Retailer model, by contrast, requires complete file tracking and end-user billing.

Nonetheless, technology already exists that can track individual watermarked and fingerprinted files.[71] Even if existing technology cannot yet perform the tasks required for the Digital Retailer model to work, the issue is one of scale rather than function. So while existing technologies may have to be improved, it does not appear that any new technologies would have to be invented.

The Noncommercial Use Levy system has all the drawbacks of the Tax and Royalty System, plus one more: it would permit users to create derivative works using downloaded digital works without the copyright owner's consent.[72]

C. Objectives Satisfied

Having ISPs serve as digital retailers achieves several objectives.

First, copyright owners would receive payment for all uses of their works—downloads, streams, and attachments—at royalty rates they set themselves.

Second, consumers would have ready, legal access to digital versions of copyrighted works, though they would have to pay for what they receive (just as we do in the physical world).

Third, website operators, P2P networks and users, emailers, instant messengers, online indexes, and search engines would be able to legally play whatever role they desire in the distribution of digital works without getting further consent from copyright owners. Online indexes and search

71. *See, e.g.*, Digimarc, Corp., *supra* note 56; Audible Magic Corp., *supra* note 58.
72. Netanel, *supra* note 16.

engines would still be free to charge for their use or sell advertising space on their display pages without sharing their revenues with copyright owners. Copyright owners would be paid by ISPs if and when works are accessed. Websites and other online services that charge users for access (like Westlaw and the online version of *The Wall Street Journal*) would have to provide something of value to justify their fees because users would be billed by their ISPs for access to copyrighted content itself. Subscribers of a pay-for-access online service may not feel they are being double billed if the service is well-organized, comprehensive, easy to use, or otherwise earns its own access fee.

Fourth, computer and consumer electronics manufacturers and software companies would be able to build and sell their products without any legal constraints on how they are designed, and without any legal requirement that they contain, or not contain, certain features.

Fifth, ISPs would gain an incentive for potential customers to subscribe to broadband service and a significant additional revenue source—one that is likely to be equal in size to the revenues received by copyright owners from the online distribution of copyrighted works.

D. Problems Requiring Solutions

Several obstacles stand in the way of successfully implementing the Digital Retailer model.

1. Technological Measures Taken by Users to Avoid Being Billed

I have argued that the technology necessary to implement the Digital Retailers model should be installed at the ISP level, rather than on users' computers, to reduce the probability of user circumvention.[73] I acknowledge, however, that determined users could nevertheless circumvent the technology.[74] For example, watermarks or fingerprints in royalty-bearing works can be hidden by encrypting those files before they are attached to emails or transmitted over P2P networks,[75] thereby preventing ISPs from billing for those works. Users may also spoof their IP addresses,[76] thereby

73. *See supra* Part III.A.3.

74. *See supra* Part III.A.2.

75. Ingemar J. Cox & Jean-Paul M.G. Linnartz, *Some General Methods for Tampering with Watermarks*, 16 IEEE J. SELECTED AREAS COMM. 587, 592 (1998) (explaining how encryption can be used to defeat copy-control watermarks), *available at* http://debut.cis.nctu.edu.tw/~yklee/Research/Watermarking/Ingemar_J_Cox/IEEE-JSAC-1998-05.pdf.

76. Neil B. Riser, *Spoofing: An Overview of Some the Current Spoofing Threats* (July 1, 2001), *available at* http://www.sans.org/rr/threats/spoofing.php.

hiding their identities from their own ISPs and avoiding payment for downloading royalty-bearing works.

The question is whether these and similar possibilities defeat the utility of the Digital Retailers model. I conclude that they do not for three reasons. First, this sort of behavior is a crime[77] or can be made one. Second, theft—for that is what this behavior would be—is a serious problem in the physical world of retailing, but no one has suggested that we should eliminate retail stores for that reason. Third, I believe that much unauthorized digital distribution of copyrighted works is currently done by people who suppose that it is legal. If users understood the illegality of encryption, IP spoofing, and similar techniques to avoid paying for copyrighted works, they would likely discontinue these practices.

2. Spamming

Since virtually all works transmitted online are eligible for copyright protection and all copyright owners would be entitled to be paid at rates they set themselves, unscrupulous authors may attempt to "game" the system by spamming end-users with unwanted material in order to get royalties. Technology may provide a solution to this problem; but if not, other non-technical solutions may be available.

ISPs' routers would be alerted to the existence of copyrighted material in files by watermarks or fingerprints before those files are transmitted to Internet users. To prevent spamming, ISPs could send pop-up notices informing users that files requiring payments are about to be sent for a certain cost before the actual files are transmitted. Users would then be given an opportunity to click an on-screen button, indicating whether or not they want the files sent. To users, the process would resemble virus warnings seen today. Users would respond, the way they respond to virus warnings, with a simple click of the mouse.

An alternate, non-technical solution may be drawn from the world of credit card fraud. In order to receive copyright royalties under the Digital Retailer model, identification information for materials sent by spammers would have to be placed in watermark and fingerprint databases along with the watermarks and fingerprints of other copyright owners. ISPs could be authorized to suspend royalty payments to those against whom spamming complaints are lodged, just the way banks suspend or revoke the credit card merchant accounts of retailers if consumer complaints are lodged against them.

---

77. 17 U.S.C. § 1204(a) (2000) (making it a crime to violate the anti-circumvention provisions of §§ 1201 and 1202 for "commercial advantage or private financial gain").

3. Intra-industry Conflicts

Implementing the Digital Retailer model also requires resolving two conflicts within the entertainment industry. The first intra-industry conflict is the result of an old but still troublesome fact: single works often embody several separately-owned copyrights. Music recordings embody at least two copyrights per track: a copyright in the musical composition, usually owned by a music publishing company (and if a song is co-written by more than one songwriter, the musical composition copyright is likely to be co-owned by more than one publisher); and a copyright in the recording itself, usually owned by a record company. As a result, royalties for the online performance or download of a single recording must be split between two or more copyright owners. In addition, music publishers grant licenses for performances and downloads through separate agencies: ASCAP, BMI or SESAC for performances; and the Harry Fox Agency for downloads. So today, royalties for the online use of a single music recording may be claimed by three separate agencies on behalf of two or more separate copyright owners.

Likewise, a movie may embody several separate copyrights: one in its visual elements and the sound effects in its soundtrack, and another in each song in the soundtrack. As a result, royalties for the online performance or download of a single movie may also have to be split among several copyright owners.

Some copyright owners may demand too much, thereby discouraging customers from making online uses of works to which those copyright owners contributed. Other contributors to the same work may be pressured to decrease their royalty rates in order to lower the total royalty claimed for that work enough to increase sales volume. The presence of multiple owners may thus trigger strategic bargaining among copyright owners, each owner hoping to persuade the others to lower their royalty demands. This process may not succeed, however, in lowering the total royalty enough to actually increase sales.

Under the Digital Retailer model, none of these kinds of conflicts is of concern to ISPs. But before ISPs can know who to pay, conflicts like these will have to be resolved.

The second intra-industry conflict involves ISPs: some ISPs and some copyright owners are subsidiaries of the same corporate conglomerate. Given complete discretion, such a conglomerate may choose to implement a business plan that seeks to attract subscribers to its ISP subsidiary by offering them exclusive access to the conglomerate's copyrighted works

or access at lower rates than those charged to unaffiliated ISPs.[78] The Digital Retailer model, however, would give all ISPs access to all copyrighted works. Also, to prevent copyright owners from substituting high prices for exclusivity, all ISPs would have to be charged the same wholesale royalty for each work. Copyright owners could not favor some ISPs with lower royalties than they charge other ISPs. This means, for example, that Warner Bros. and Time Inc. could not charge their sister company America Online lower royalties for digital recordings or online magazines than they charge other ISPs, let alone give America Online exclusive access.

4. Privacy

The Digital Retailer model requires copyright owners to make significant concessions of control over how, when, where, and to whom their works are distributed. It also requires some concessions from users. For example, in order to enjoy the convenience of online access to copyrighted works, users will have to tolerate some loss of privacy. The Digital Retailer model requires ISPs to compile records of copyrighted works accessed by their subscribers for billing purposes.

Some may view this as an unacceptable loss of privacy.[79] I, on the other hand, see this as a small and acceptable loss of privacy when compared with the other invasions of privacy people accept today. Credit card companies already know where we shop and how much we spend. When we shop in places or spend amounts that look unusual, they call us on the phone to confirm that our cards have not been stolen. Likewise, phone companies already know who we call, when we call, and how long we talk. Even our patronage of brick-and-mortar retail stores is likely to be videotaped.[80] And in many American cities, highway and toll bridge users and their passengers are likely to be videotaped as well.[81]

In sum, The Digital Retailer model is no more intrusive than credit card or telephone company billing schemes. Tracking copyrighted works

78. Reuters, *AOL to Offer Exclusive Time, CNN features* (Dec. 3, 2002), *available at* http://www.ispworld.com/Reuters/BreakingNews/120302_js04.htm.

79. *See, e.g.*, Julie Cohen, *DRM and Privacy*, 18 BERKELEY TECH. L.J. 575 (2003).

80. *See, e.g.*, Tim Coyne, *Videotaped Beating Mom Pleads Guilty*, CBSNews.com (Feb. 14, 2003), *available at* http://www.cbsnews.com/stories/2002/09/20/national/printable522684.shtml.

81. Paul W. Shuldiner & Jeffrey B. Woodson, *Acquiring Travel Time and Network Level Origin-Destination Data by Machine Vision Analysis of Video License Plate Images*, Presentation at 1996 National Traffic Acquisition Conference, at 442, *available at* http://www.itsdocs.fhwa.dot.gov/jpodocs/proceedn/2g901!.pdf.

we access online, for billing purposes, diminishes our current levels of privacy only slightly.

5. Pay-per-use, Fair Use, and Non-infringing Uses

Some may object to the Digital Retailer model because it requires a pay-per-use royalty and makes no payment exceptions for non-infringing uses, including fair use.[82] But this objection is accurate only in part and is no reason to reject the model.

The Digital Retailer model does not require payment for each *use* of a work. It requires payment each time a work passes through an ISP's router. Thus, rather than characterizing the model as a pay-per-use model, it should be thought of as a pay-per-redistribution model. Downloaded works may be used countless times on the computer to which they are downloaded without additional payment. Only the initial download triggers a royalty fee.

Those raising the non-infringing use objection imply that users should be able to get free access to copyrighted works they intend to use in ways that qualify as non-infringing. That, however, has never been the case in the physical world. Teachers, for example, may be entitled to display or even photocopy newspaper articles for use in their classes, but they do not have the right to take copies of newspapers from the newsstands they pass on their way to school without paying. Likewise, movie critics have the right to include plot synopses and quote dialogue in their reviews, but they are not entitled to free admission to movie theaters showing the movies they intend to review.

6. Unregulated Royalty Rates

I have left the lack of regulation of royalty rates for last because for me it is not a problem at all. I acknowledge, however, that for others, lack of regulation may be troubling. One might argue that copyright owners may effectively eliminate the ability to legally reproduce copyrighted works and redistribute them online by charging high rates.

While copyright owners may charge high royalties for some works, especially when they are new, they always have had the ability to do so in the physical world. A recent report entitled "Digital Rights Management: Content Protection in the Networked Economy" has been priced by its publisher at $995,[83] and newsletters published by the same company cost

82. *See, e.g.*, Raymond Ku, *Consumer Copying & Creative Destruction: A Critique of Fair Use as Market Failure*, 18 BERKELEY TECH. L.J. 539 (2003).

83. *See* Kagan, *Kagan Catalog*, *at* http://www.kagan.com/cgi-bin/pkcat/drm03.html (last visited May 3, 2003).

more than $1,000 a year,[84] without apparent objection from anyone. There is no reason why things should be different—especially not by law—in the digital world.

Nor is there any reason to suppose that copyright owners would set high rates to eliminate digital versions of their works altogether. Naturally, when motion pictures are first released to movie theaters, or television programs are broadcast for the first time, their owners will not be pleased by online distribution of unauthorized copies. As previously noted,[85] distributing unauthorized copies online shortly after a work's first release interferes with the owner's ability to engage in sequential and separate releases of that work. Copyright owners may therefore set high royalty rates for newly released works to discourage the online distribution of unauthorized copies at that stage. However, by the time movies and television programs are made available on DVDs, copyright owners have no reason to prefer DVD distribution through retail stores to online distribution through ISPs, so long as their online royalties net them the same amount per download as they net from the wholesale price of a DVD.

IV. CONCLUSION

In a perfect world, technology companies and copyright owners would have complete freedom to design and market their products as they think best. Digital copying and redistribution have made these objectives incompatible, at least in part. The quest is for a business model that best accommodates these conflicting objectives.

As a general rule, copyright owners are opposed to statutory licenses.[86] Some copyright owners may object to the Digital Retailer model as being a statutory license and will be hostile to it for that reason. Their freedom, however, to set their own royalties should soothe this objection. Still other copyright owners may contend that the Digital Retailer model—tied, as it is, to online redistribution—will simply promote unlicensed and uncompensated CD and DVD burning and a return to the "sneaker net" of disks and tapes that "were handed in person between members of a group or

84. *See* Kagan, *Kagan Catalog*, *at* http://www.kagan.com/cgi-bin/pkcat/scan/se=usnews/sf=pk_item/se=hardcopy/sf=pk_sort/tf=title.html (last visited May 3, 2003).

85. *See supra* Part II.A.

86. *See, e.g.*, *Napster, Music Industry Square Off on Capitol Hill*, USATODAY.com (Feb. 6, 2002), *available at* http://www.usatoday.com/tech/techreviews/2001-04-03-napster.htm; *Statement of the American Society of Composers, Authors and Publishers on Internet Uses of Music for the Senate Judiciary Committee Hearing on "Online Entertainment," available at* http://www.copyrightassembly.org/briefing/ASCAP2.pdf.

were sent by postal mail."[87] Indeed this may occur; if it does, the issue of blank media levies will again take center stage.

The Digital Retailer model will likely draw objections from consumers and their advocates. Hardware and software companies would be relieved of all burdens by the Digital Retailer model. And ISPs should be pleased with their share of the retail take. My concern is that even if the implementing technology works perfectly so that consumers are charged only for what they choose to buy and only at prices they have agreed to pay, they or their advocates will view the Digital Retailer model as one that gives copyright owners too much control.

Any argument that copyright owners would have too much control, however, is one that would overstate the extent to which copyright owners have exclusive rights to their works. Copyright law gives copyright owners very thin protection. It does not protect ideas, concepts,[88] theories, or the facts on which they are based.[89] Thus, although "Mickey Mouse" belongs to Disney, "Mighty Mouse" does not; "Mighty Mouse" belongs to Viacom.[90] And while copyright law does not permit others to make exact copies of "Mickey" or "Mighty Mouse," it does permit unregulated breeding of other animated mice by all who wish to do so. The thin protection of copyright law does not even give anyone the exclusive right to tell stories about archaeologists in search of artifacts hidden in snake-infested caves while simultaneously confronting dangerous human antagonists. Anyone who wants to tell that story, may.[91]

Finally, in the music business, copyright law does not give record companies the ability to obtain exclusive recording rights to songs. Instead, all who want to make and sell their own recordings of popular songs, even sound-alike versions, may do so simply by paying license fees to music publishers at rates set by law.[92] MP3.com could have started its own record company—producing sound-alikes or original recordings—for less money than it agreed to pay in settlement of copyright infringement lawsuits filed against it by record companies.[93]

---

87. Biddle, *supra* note 61, at 3.

88. 17 U.S.C. § 102(b) (2000).

89. Hoehling v. Universal City Studios, Inc., 618 F.2d 972 (2d Cir. 1980), *cert. denied*, 449 U.S. 841 (1980).

90. Search for "Mighty Mouse" at http://www.copyright.gov/records/cohm.html.

91. Zambito v. Paramount Pictures Corp., 613 F. Supp. 1107 (E.D.N.Y. 1985).

92. 17 U.S.C. § 114(b) (2000).

93. *MP3.com Settles Copyright Case Filed Against it by Universal Music Group by Agreeing to $53.4 Million Judgment*, 22 NO. 6 ENT. L. REP. 5 (Nov. 2000).

There has been debate over the appropriate scope of the derivative work right: the right to make new versions of copyrighted works.[94] But the derivative work right is not at the heart of the digital copyright controversy. P2P and related controversies have involved digital copying and online redistribution of exact duplicates of copyrighted works.

Given that copyright law permits anyone to breed new animated mice, tell new stories about adventuresome archaeologists, and make new recordings of "Oops! I Did It Again" using vocalists who sound just like Britney Spears, it hardly seems too much to ask that they do so, rather than make unpaid-for digital reproductions of works whose copyrights are owned by others.

94. *See* 17 U.S.C. § 106(2) (2000); Suntrust Bank v. Houghton Mifflin Co., 268 F.3d 1257 (11th Cir. 2001); Castle Rock Entertainment, Inc. v. Carol Publishing Group, Inc., 150 F.3d 132 (2d Cir. 1998).

EDITED & EXCERPTED TRANSCRIPT OF THE SYMPOSIUM ON THE LAW & TECHNOLOGY OF DIGITAL RIGHTS MANAGEMENT

TABLE OF CONTENTS

I. INTRODUCTION

On February 28 and March 1, 2003, the Berkeley Center for Law and Technology and the *Berkeley Technology Law Journal* presented a symposium on Digital Rights Management. The following are edited versions of the transcripts from several of the conference panel discussions. Full transcripts are available at http://www.law.berkeley.edu/institutes/bclt/drm/transcriptions.html (last visited Apr. 24, 2003).

II. IMPACTS OF DRM ON INNOVATION, COMPETITION AND SECURITY

Panel:

Hal Varian, School of Information Management and Systems, University of California, Berkeley (moderator)

David Farber, Computer Science, University of Pennsylvania

John Manferdelli, Microsoft Corp.

Lucky Green, cypherpunks.to

Alex Alben, RealNetworks, Inc.

VARIAN: John Manferdelli will speak on principles guiding trustworthy computing, kind of lay out some of the technology and some of the principles that should apply. Lucky Green will talk about who the computer should trust. And Dave Farber will talk about some of the privacy and security of the digital rights management issues that arise in the technology. Then I'll chime in and say a few words about some of the economic and business issues, and then [Alex Alben] will wrap up with some discussion of government policies towards DRM.

MANFERDELLI: I'm going to talk about the principles of digital rights management, and I'm actually going to follow up on a theme that Allan [Adler] mentioned, that it's not exactly one size fits all.

We think of rights management as a way to have rights persist with the thing they're trying to protect. That's lots of stuff. It's to protect and to share assets both with customers, vendors, and other employees. It's also to protect personal information, personal photos. So there's a wide range of things not only in the pure commercial space, which I think most of the discussion has focused on today, but in other spaces. And all the attack models you have to think about it in each of the domains carefully that what you are trying to do is very different in all of those domains.

So, one of the areas which most people spend all their time doing, which I think of as classic DRM, is audio-video protection. And that's basically people thinking: "We're going to sell audio files and video files to people over the Internet."

So it is not the purpose of a DRM system to have provided a perfect protection mechanism. In fact, it cannot ever possibly do that. I guess there's some question as to whether any system could possibly do that. But let's look at a very different application. I think last week we announced something we call "enterprise rights management," and that's to protect documents for a corporation. And there, the issues are completely different. Privacy issues are much reduced and what you think of as "fair rights" doesn't come into it. It's roughly the same technology. It's basically a way to authenticate the thing you're granting rights to and authorize it, but it's a very different application domain.

Personal rights management can be two fold. And then finally, privacy rights management, from trying to protect my e-mail or documents to having a conversation with my lawyer or my doctor that's a very different kind of protection that has a very different attack model, and what you're trying to prevent is actually quite a bit different.

People who were clearest about what they wanted and wanted it right now were in the enterprise. So we have done audio-visual video protection systems. Intel has a very clear focus, and the focus is not to restrict what people can use their computers for. We don't want to restrict it in any way. What we want to do is enable new stuff. And we want to enable them to get things on their computer that people would be unwilling to let them have now, or would not risk, in the situation PCs are used in right now.

So I think one sort of key aspect, and I think something nobody is sort of focused on in a very clear way, is whatever the mechanism you use, it cannot impose policy. It's very difficult to anticipate the policy needs of a

DRM system. They change all the time, and they change with application, so whatever the system is, it has to have this sort of 360 degrees of policy. It has to be an "opt in" model. One of the issues with mandated DRM is users don't have the option to decide whether they want it or not. And one of the firm principles is it really ought to be in user control. That is, the user ought to decide whether he is willing to go along with this.

It really ought to benefit both the corporation and the user. I expect it to evolve over time, and I expect that will be a matter of negotiated equilibrium. As a technology provider, I can't be in the middle of that. It just won't work for two reasons: One is it'll take me six months, a year, to get out the next release that does the next thing you want in policy management; and the other reason is that you won't trust me to do it. You have to be able to specify what you want and get that to happen. So, I do think much of what we talk about, as it settles down, is going to be a matter of negotiated equilibrium in the application spaces that the DRM or rights management systems are used.

I think there are some principles that go along with that. Don't censor or disable content. Stuff that works on a PC now, it's a bad idea to go around and try to disable it. That goes against the principle of enabling your stuff, and if you ever blow it, you're in deep trouble. The intention is not to lock out the vendors or format. In fact the whole idea is the DRM layer ought to be interoperable in that 360 degrees of policy dimension. There ought to be a standard to say what you want, and have it both be extensible when you think of new stuff, and have it enforced whether it's your technology or not that's doing the enforcing.

With end user control, one of the common questions is, "Who owns the key?" and the answer is, "Nobody." The machine acts on behalf of the user. If the user allows a certain set of operations to take place protecting a certain set of content, it does that. If the content is the user's content, it acts on behalf of the user. If it's somebody else's content and the user said, "Go ahead and protect it the way I've agreed to," it acts on behalf of the user. But there's no key that's owned by somebody. There ought not be in such an operation.

It won't be perfect. It can't be perfect. Bob [Blakley] is right. There's a sort of famous guy I like a lot at Microsoft called Butler Lampson who, one of his favorite aphorisms is: "the enemy of good security is the demand, not the quest, for perfect security." All these systems are trying to do something. None of them are trying to achieve perfect security. They're trying to provide a benefit, some sort of describable benefit, for the people who use it. In the case of enterprise documents, that's to keep documents from leaking, either accidentally or, in some cases, on purpose. In the case

of video, and for consumers, it's to try to have a reasonable sales model so that people can: (a) use their PCs to do what they want, which sometimes, believe it or not, is to look at videos, and (b) not destroy your entire business model. So it won't be perfect.

I've heard two comments on the "DarkNet" paper, and I do want to correct a couple of almost misimpressions. The purpose of the paper was not to say, "DRM, you should just abandon it"; nor was it to say, "You shouldn't do enforcement on a client machine." There are lots of reasons you want to do that, just for pure computer science reasons. There are a lot of things you do which you may or may not think of as DRM. The purpose of "DarkNet" was not to say that DRM wasn't useful in all these domains; it was to say, "Wake up, be realistic." If you're selling a book, realize that somebody could type the book in. Arguing over whether the system was perfect was a little bit useless because there's already a medium for injecting that content into the Internet, and you don't solve it simply by doing client enforcement. And in fact, the best thing to do is offer customers good legal, reasonable choices, probably with DRM, maybe without it.

So there are a lot of models this enables, and I want to make a slightly arrogant, technical statement and a very humble policy statement: I think we can build systems that give the user control, that let people achieve this negotiated equilibrium, but I don't think, as technology providers, we know the answer to how the policy is going to evolve. That's my key message, and that's the thing I think has driven most of our designs: it's policy neutral. The person it's protecting is the person it's protecting, and it won't do that unless the user says so.

GREEN: I would like today to focus on one aspect of digital rights management and its bigger and somewhat meaner brother, trusted computing. One of the subjects of my talk here is whom do you trust and why should you trust entities that perhaps may not trust you.

Let me tell you a story. In the fall of 2000, I worked at the time for a fairly sizable vendor of security products used throughout the industry and received an invitation from this new association that I'd never heard of called The Trusted Computing Association. It sounded really good. What this invitation said is that, "Hey, we would like you to join us; we've been founded by some of the largest players in the computer industry, and what we would like to offer you is 'secure boot.'" Now "secure boot," as I understood it at the time, would enable my applications that are running on top of an operating system to not just know what operating system they are running on, but also what is running underneath the operating system. For example, has my hardware been compromised given the applications that we did? This seemed quite important.

I attended some of the formative meetings, and at one meeting, one of the founding principles of this Trusted Computing Association, TCPA, after we were discussing secure boot, said that one important thing you need to remember is that they were not building a DRM system. Why was he talking about a DRM system when we were here to talk about secure boot? I let it go for a moment, but a few minutes later, he again said, "It's important to prevent the public from thinking that we are building a DRM system." After two or three such remarks, I started to wonder, "What is going on here; what are these people really up to." During a break, I took aside one of the other founding members of the Trusted Computing Platform Alliance and he told me, "Listen, it's very simple. Our operating system platform, on a general peer purpose PC, currently does not have server content available, such as, for example, high quality streaming video, that our customers demand. The content owners, or I should say the accumulators and distributors, have told us that they will not make this content available until such time that we have these features available on our platform. We don't have much of a choice. We have to solve this problem one way or another." While I understand that the future for digitally released content, certainly in the home environment, is of importance to future business models, it still didn't quite explain to me why some of the largest companies in the business here not only were in the process of implementing new hardware-based digital restrictive management technology, but actually at this point in time really had conspired to keep the public and the customers in the dark about the true purpose, which was DRM. I'd like to address some this today because after a few years, I and some of the others in the industry believe we finally figured out why.

First, however, I need to somewhat definitely define what the word "trust" means when used in the context of "trusted computing." It does not exclusively mean that you as the owner can trust the processes running on your machine. It also, and perhaps for the purposes of our discussion today, more importantly means that third parties can trust that your computer will disobey your wishes. Third parties by means of trusted computing will know that your computer will implement whichever digital rights management system the producer of the content has placed on the content. The analog to this in the analog world, as opposed to the digital world, will be that a book vendor will know that you can read a book only once, and then only with a special light that they will also happily sell you.

However, that is certainly the classic DRM application. There is another side to this. Providers of trusted computing products, especially if they're in a dominant market position, can trust that potential competitors will be prevented from competing in the future ever.

Some of the obvious business objectives of trusted computing and the DRM it implements are, of course, the usual: prevent CD ripping and Divx creation. Something that hasn't been talked about much is the plugging of the analog hole. What's the analog hole? Well, today's computers are high quality. Even with the best digital rights management system, you can still feed the speaker output right back into the sound card and digitize, which will give you a darn good copy, one that will certainly sound fine on the computer speakers on which most people probably listen to their MP3s.

Another issue is enabling flow control, information flow control, which I won't get into today. It allows the application provider to prevent the use of unlicensed software. Now this is something of more interest to application providers, if you're an application provider. It thereby, as this gentleman from this operating system and office productivity company told me, will allow the PC to become the core for home entertainment center, growing a new market. The PC industry fully understands that at the core of your future home entertainment system there will be some device processing data, and that device can either be manufactured in a PlayStation-like fashion by Sony or it come from the usual vendors in the PC industry. The PC industry does not want to lose this market to Sony. They need to compete and this is fairly understandable.

And lastly, it creates new market opportunities in the governmental sectors. Government employees are notorious for leaving laptops with top secret data on buses and in train stations. This is repeatedly being reported in the press. Having hardware security that prevents third parties from getting at this data obviously is a good thing and a clear and very legitimate market for it.

So, let's look at some of the upcoming hardware/software DRM features in office productivity software, and here I would like to quote Bill Gates from Microsoft, "We came at this thinking about music, but then we realized that e-mail and documents were far more interesting domains." Why is that? Rather than hoping for a potential market expansion in the home entertainment system market, there certainly is a current clear market for office productivity software—Word documents, e-mail documents, what have you—and there is at least some demand, and certainly some vendors believe there is a massive demand, for this technology. For example, you can't forward this Word document outside the company or, I should say, you can perhaps forward it, but nobody else at the company will be able to open it. Or you have some e-mail that only can be displayed on your screen and by the way, we're disabling screen copy so you can't just dump it to a graphics file. Or a document as was also stated would only be valid for so long, and then will no longer be readable regardless of

what PC you copy it to because you have a secure clock, there's no such thing as setting back the date.

If you are the CEO of Enron, you would just absolutely love this technology, because there would be no evidence left for discovery. So yes, there are clear benefits. It's not clear that these are clear benefits to society.

Question: what does the federal prosecutor call a third party application that is compatible with the proprietary DRM format? An illegal circumvention device. If you build compatible software that can read a DRM wrapped file format, you, at least as long as the software is open, thereby enable third parties to infringe on such digitally rights-managed content. One hypothesis, and certainly my hypothesis and I believe it is the vendor hypothesis, is that this will make it illegal to create interoperable software in the United States, interoperable with software that has DRM features enabled subjecting software authors to substantial penalties. So what are the choices? Don't create interoperable software or spend five years in prison. As a product manager for software, this does not sound very appealing.

Lastly you will hear that DRM is voluntary. That is absolutely true. It will be voluntary. You do not have to turn on your computer; you do not have to power it up; you do not have to read the documents that are DRM wrapped and that will be sent to you, which if it becomes enabled in office productivity software, of course, will be something that you will probably have to do to do your day job; but you don't need to do that. Nobody is forcing you with either the law or physical force. Thank you very much.

FARBER: Let's start with some miscellaneous comments just while I have the microphone. One of the things I think we've suffered incredibly from is having a marvelous religious war and not paying any attention to understanding very clearly and articulating what the technology is capable of doing, what it isn't capable of doing, what its limitations are in a technically valid way, and instead arguing that the world is going to collapse or the world will be sunny. It is real good for some newspaper reporters but it doesn't help at all in understanding really where we are. I recommend strongly we stop having religious discussions for the time being, at least.

The other observation, for those who don't have historical perspective, is rights management is not a new idea. It's been tried ever since I've been in the computer business, and I go back quite a ways. It's always suffered from the fact that, in general, it's been a software product, and software products are easy to break, very easy to break. That means that in fact they've been not very useful things.

A couple of systems have hardware protection. Luckily or unluckily, take your choice, they never quite made market. Certainly when we designed the original Motex system, that was an issue. It wasn't rights management. It was protection of documents, protection of private information.

I was an advisor to TCPA since its beginning. Along with some other people, I have no benefit from it, I haven't even gotten a trip out of it, but I had some interesting discussions in the very early days. Let me make two other comments while I've got the microphone and then I'll get to the meat.

The ARPANET was not built to survive a nuclear attack and I wish people would stop saying that. It would not. And finally, anybody who would like the FCC to be in a regulatory position of new business models deserves what they'll get. I served there for a year and a half, and tomorrow, in fact, we're having a conference down in Stanford, for which the intention is to get the FCC out of the spectrum-regulatory thing.

Let me punch in some stuff. I'm not going to spend a huge amount of time. A lot of what I was going to say has been well said, but I think it is important to push down on the issue of security, and I understand, the lack of perfect security. If we look for perfect security, we'll be here for the next five hundred years. However, an acceptable level of security is getting more and more important in the world we live in. It's important for individuals, it's important for corporations, and it's going to be increasingly important for nations. Things which increase the level of security are very hard to turn down, realizing that of course they're never perfect.

When you have a relatively secure system, I would hold that it is very difficult for you to keep out a rights management system, especially if you don't own the machine down at the gut level.

But in fact if you have anything other that boot privileges, the equivalent which most of us have, it's reasonably hard to not host the rights management system. If you say by law somehow that you can't implement rights management, you are essentially saying by the time you're done that you are not going to be able to build or at least market a secure system, and I think that's a bad trade-off. The details of that, I think, deserve study and deserve careful looking at.

The other thing that I'm less interested, and always have been less interested, in is protecting media companies against people "illegally" using their material. I would never do that, of course. But I am very much progressively interested in having people not gain access to my personal in-

formation, and that is getting to be a serious problem, and it's going to be an even more serious problem in the future.

And protection mechanisms—and I'll avoid the words "rights management"—have a very important goal in protecting my information, and being able to find out who's looked at it, who's made copies of it, who's passed it to whom. The same type of stuff the media companies claim they would like to know for their own market purposes, I want to know for the protection of my own data, and I want mechanisms which enable me to do that. Whether those mechanisms are used by other things is going to be an interesting issue that's going to have to, at some point, be decided by legislatures, by courts, and the marketplace—you don't have to buy it.

Down at the FCC, I spent a fair amount of time being in the middle of long discussions about the other type of rights management, things that sometimes show up as broadcast flags and other various schemes designed to protect the transmission of high quality digital video largely—the Disney problem, I used to call it, or sometimes the Mickey Mouse problem. I certainly do not speak for the FCC, but there was a terrible tendency for people to walk in with technologically inferior solutions, solutions that often when you looked at them, you asked, "Well, how good are these?" In fact, I remember one conversation, "How good are these solutions?" Answer: "Pretty good." I come back: "Nine months to break." "Mmm, maybe six." That type of solution, when put on the marketplace just causes a conflict, causes the FBI to be engaged in trapping people or arresting people. The unwillingness of the media companies to pay for good protection, assuming that we want it, and assuming they want it, is distressing because it gives you these Mickey Mouse solutions. I strongly think that that is a serious, serious problem.

I'm not recommending we have rights management systems. I'm just trying to lay out the framework. But I think the exploration of just what can you do in rights management systems to give us maybe better fair use than we have now, at least in the media stuff, might be an interesting place to do some research, maybe, and some explorations, and to articulate what we find, as technical people, down to the policy arena in Washington, where, believe me, there are precious few technical people. Thank you.

VARIAN: I'm going to spend a few minutes talking about some economic issues in DRM and basically I just want to lay out some points for discussion. I'm not going to express any strong opinions here, but I'm going to try to bring out some phenomena that I think are interesting.

One is: we have heard a lot of talk about business models, and the question is: What are the business models that are out there? These are the seven that I know about. So one thing you can do is you can advertise

yourself—that's the Grateful Dead model—give away the music in order to sell the concerts.

Or you can advertise other stuff, and that's, of course, what most media does—radio, TV, newspapers, magazines, and I include product placement where you try to integrate the ad so completely into the content that they can't really be separated without destroying the content. I actually think that's one of the stronger forces that's at work these days, and we're going to be seeing a lot of experimentation with product placement in the next year or two.

Bundle the content with other things, like t-shirts, prizes, liner notes, chances to win a talk with a band, or whatever. There's all sorts of ways you can take products that are apparently scarce, bundle them with the product that is inherently not scarce, and then charge for the bundle.

Subscription, versioning, non-linear prices are all ways of dealing with something other than a paper use or paper piece structure, and it's attractive because from the viewpoint of economics, what's interesting about information booths is that they have zero marginal cost, so you'd like to have a zero marginal price, and there are various ways you can do that, from an economics point of view.

You could just have much lower prices and higher quality for the legitimate version than for the illegitimate copies, and we've heard some discussion of that, as well.

Micropayments is another thing that I think people are very skeptical about these days, and when you have technology that enables micropayments, like cell phones which allow for the billing as part of the service, then you see a lot of content that can be offered there, and we've seen that happening particularly in Japan.

Finally, the digital rights management which is controlling the terms and conditions under which the product is consumed.

So that's my list of seven. I think it's important to start thinking about these business models, and really laying out what their pluses and minuses are. For example, there are a lot of bad things about product placement as well, but still, it's something that enables certain kinds of behavior.

Now when we look at this digital rights management and the choice of terms and conditions under which the product is consumed, it's important to understand that a rational seller, profit maximizing seller, will want to choose the bundle of rights that maximizes the value of the product, not maximizes the protection; and the trade off here is that the more rights you give the consumer, the more valuable the product is to the consumer, because they can do more things with it. But of course, it may be that you

have fewer sales because of leakage and sharing and copying and other things like this. So the trick is to choose the right tradeoff for libraries, for-profit libraries sprung up in England in the mid-1700s and early 1800s. The publishers hated this idea; they thought it was terrible that you would have these libraries spring up and of course, the availability of the low cost literature increased literacy, increased the number of habitual readers, and created a much larger market than they'd had before. Pretty much the same story happened with the video machines, a couple of hundred years later, where there was a lot of fear and loathing of video machines. Of course, we all know that's created massive new markets. When the DVD came out, it was quite interesting that the DVD was targeted from the very beginning at a purchase market, to make the price low enough to discourage rebels and encourage purchases and the DVD has been a hugely successful technology, in part, because of the economic model that they used.

. . . .

The point is if you sell it for a high price and it has a lot of rights, well then, the trouble is you might increase the incentive to try to share among consumers in that context. So the lesson is that cripple-ware is not the best thing to do necessarily. It inherently reduces the value of the product, and of course, it's easy to compete away copy protection. So whenever you do have a lot of competition out there, as we do in content provision, it's very hard to enforce solutions that inherently make the product more difficult to use.

Now, I want to say one last bit about innovation because innovation is in the title of this meeting. There are very interesting kinds of protection out there, not just for information, but for other kinds of physical products. For example, Epson makes a printer that has an inkjet cartridge. The inkjet cartridge has a chip in it, and the chip says, "You can't refill me." It'll count down, when the ink is all gone, and when the ink is all gone, it can't be reused. Now actually, on the Internet for twenty-five bucks, you can buy a device that will reset this chip. Motorola makes a cell phone that only allows certain batteries, it has to be a Motorola battery, because it has a chip in it that says, "I only want to connect with Motorola phones," and Motorola phones only want to connect to this battery.

But then there are interesting innovations around each of these technologies. We have some people over in computer science and electrical engineering who are printing integrated circuits using off-the-shelf inkjet printers with magnetic ink and metal-coated plastic. So you can just take an off-the-shelf ink jet printer, hack at it a little bit, modify the ink and print out integrated circuits. So it's quite a nice technology, and can totally change the economics of that business if they can ever get it to work suc-

cessfully. There are some people who are making generators in your shoes, so you walk along, and you can charge up your cell phone, and charge up these other devices. Just put a little generator in your heel, and as you walk around, you can create a charge. And finally, the last example is: last summer in England, the number one song in most of Europe was this thirty-year-old B-side single from Elvis called "A Little Less Conversation" that Nike had used in its sponsorship of the World Cup. This had been re-mixed by a Dutch disk jockey who added some techno beat to it and made this new kind of music that people really loved.

Now, each of these technologies, each of these innovations, would have been very difficult to do if you had really perfect copy protection. If you have these non-refillable ink cartridges, you can't adapt them to different purposes. If you have these cell phones that only accept certain batteries, then you can't build this charger that runs through walking around, and if you make it very difficult to rip the CD, then you can't modify the music, update it, change it, and use it as an input to further innovation. One of the best things you can do as a business is try to draw on your user experimentation. There's a very nice set of work by Erik von Hipple at MIT about how strong this force of customer innovation is, and he has dozens and dozens and dozens of examples where you learn a lot about how your product can be used by making it, by providing tool kits, and making it easy for people to modify it; and so if you restrict the way products are used, in some cases, you can lose the benefit of that kind of innovation. So that's a danger that may be outweighed by other benefits, but it's just something people should be aware of.

. . . .

ALBEN: I'm Alex Alben with RealNetworks. I'll start with a confession, which is, when I took real property from Paul Goldstein down at Stanford, he spent the first day of the session talking about a bundle of sticks, and I didn't understand. I was thinking of real property, and he kept talking about sticks, and it actually kept me, for the next 20 weeks, stymied. I wasn't able to get to springing rights and flowing rights and the other things, and I ended up not doing very well in the class, which led me to my career, ultimately, in the software business, where we don't deal with real property. But it really came home to me that what he was talking about in that first class of real property was that intellectual property can be split into bundles of sticks; and I think we should change the metaphor for our world into bundles of splinters, because you can take the digital product and obviously parse it in the ways I'm suggesting. Now this has come into conflict with people's expectations of property and copyright, because when you buy a CD, you don't think about, "Well, I'll only use

this CD and this one CD player," or "I'll only use my CD on Sundays, and that's the only time that we'll play on this device," or "I'll only play it three times and then it will disappear." Actually it will still be locked onto my hard drive, but the rights to it will disappear and I'll have to circumvent and commit a crime in order to listen to it a fourth time. This has become a very real problem for our society, and, I think, for the industries that are thinking of building this digital marketplace. And I'll be a little less abstract than some of the other presentations and talk about the problems that we've encountered in the real marketplace, the early marketplace, for creating digital distribution of media.

I have a thesis, which is that we need to maintain both a personal use right and copy protection in order to build a marketplace that works. Now, we know that DRM enables business models, and Hal [Varian], I think, did a good job with some creative examples of business models and price points. It's happening with music subscription and video subscription in an early way. It's happening in general entertainment for some products that we and other companies have put out.

The problem is not so much, "Is there DRM technology." We don't pretend to have a perfect DRM, and if anyone sold you a perfect DRM, you should probably pay at least a dime for it. We have a reasonably good DRM that is protecting content in the marketplace, making it difficult for the average user to circumvent or break the DRM, therefore supporting the business model and the price point. If you're offering something for $10 a month, you might not need a DRM that a team of scientists led by Ed Felten, or somebody at Berkeley, could spend, three months with 12 supercomputers arrayed and eventually break. It would be easier, maybe, to go and spend the $12 at Tower Records. So, we have a reasonably good DRM, and there are other companies in the market place, such as IBM, such as Microsoft, InterTrust, who also have reasonably good DRMs for the purposes that the content is being distributed for today.

The issue, I think, is not whether the consumers are enabled or whether the technology exists, but one of the issues is, "What's the price point?", because we have split the bundle of sticks into the bundle of splinters and toothpicks and other things that consumers no longer recognize. What's the price point of a 30-day download that's tethered to a single computer? Now we've run into this issue directly with MusicNet and some of the other services that we've brought to market. If you talk to the music publishers, the people who administer the rights in the composition that is embodied in the sound recording that is being distributed in that digital download, they'll say, well, it's about seven and a half cents. Funny that

they should come up with seven and a half cents because that is exactly the same price that they get when a CD is sold.

Now you can say, "Hmm, do we live in a parallel universe?" A CD has a lifetime of what? Let's say 10 years. It's really, you know, until somebody in your house scratches it or you lose it or you move, but 10 years with how many unlimited number of plays? How many months is 10 years? 120 months, right. So, you're getting 1/20th of that value, and of course, you can only play it on one device in my scenario. So let's say you discount it further, so maybe you should pay 1/240th of the price of seven and a half cents. I'd say that's reasonable. At least that's supported by the differences in the technologies, but if you talk to some of the publishers, they'll say, "Well, we'd be happy to license this to you, but at seven and a half cents per copy per month."

I want to talk about what we need to build the marketplace, which doesn't involve everybody taking. It actually involves everybody giving a little to make it work. For content owners, not just the record industry, but the entertainment industry and anybody else who has valuable content to protect, I think the requirement is that they put the product into the marketplace.

And in order to effect the licensing of that product, we need licensing mechanisms that allow for mass distribution of content. I'll pick on the music publishers again because after a time, the tech industry, with Microsoft and RealNetworks and others, was able to convince record labels and work with them in partnership to create some systems. You can say they're imperfect; you can say the rights aren't there. You can say the Beatles aren't there—and I wish they were. But the problem is that another set of rights was necessary for licensing, and if you address the music publishers, they'll say, "We're happy to license this to you. Give us the form." We'll say, "Well, we have 100,000 songs we want to license tomorrow." "Well, we can't accept that in electronic form." "Well, can we send you a spread sheet?" "We're working on that." "What do you want to do in the meantime?" "Well, could you send us some written, per request of what you need to get per song, and then we'll try to identify the rights holder."

I said, "This isn't going to scale." We have the rights already to distribute 100,000 songs from the labels, but we don't have a licensing mechanism that is easy enough to support the business model that we have built. And this, I challenge the audience, is where we should pressure our legislators to actually do something. It's worthless to create a quasi-compulsory license for one half set of rights without another compulsory license to affect the purpose of that compulsory license.

Maybe we don't have to call it a compulsory license because that's a loaded word. Maybe we should call it a safe harbor. Maybe we should call it a notice provision. Whatever it is, we want to pay the songwriter. We want to pay Lennon and McCartney, or Michael Jackson or whoever owns that catalogue of Beatles songs. And we're willing to put money into a pot, but what we want to say is, we want to put this in the marketplace tomorrow so that then we can collect the revenue and divvy it up according to usage. It's an important gating item for this marketplace to work.

Consumers have to use products in ways that are consistent with personal use. If I went to my neighborhood in Seattle, and took my CD burner and had a stack of 1000 CDs and stood on the corner and put up a sign that said, "CD Burns Free," everyone would come by. I'd just say, "Here's the CD. There's one for you and one for you and one for you." Eventually I'd cause a traffic jam, but the point is it's not legal activity within the scope of accepted personal use, and file sharing to 1000 people that you don't know is also not personal use. We need to disabuse ourselves of a concept that just because the user may not know that the default setting on their PC is to share to the rest of the world, that that is somehow justified behavior. It isn't justifiable behavior. If consumers want a reasonably placed product in the marketplace, if they want to encourage content providers to put that product in the marketplace, then they need to act in a way, we need to act in a way, that's consistent with our traditional rights in personal use.

Tech companies, we need to enable the business models, make DRMs transparent to consumers and not make them jump through 12 hoops in order to authenticate content and get rights.

For the government, we would say, and I'm really happy that RealNetworks and Microsoft and Intel and other companies will violently agree on this point, please don't regulate this industry, please don't mandate, and please don't choose winners. That is not a formula for innovation. You know, the government in India has the spec for automobiles, and they say in India you can buy the best 1950s car on the market today. We need to live in an industry with a vibrant society, creating new technologies, and constantly innovating. It's not going to happen if we have to go to an FCC rule-making every time we need to change the spec for a product. To thinkers, such as people in this audience and the people who put together this conference, we need to create this intellectual framework for the new paradigm.

What are the challenges that remain? Crafting a fair use exemption for distribution of a circumvention tool that does not swallow the rule. This is a hard problem. I don't know how to figure it out. I would love for a prod-

uct of this conference to be a variety of proposals and papers that allow this.

The second is limiting application of the DMCA to protecting valuable media. Was the DMCA intended to protect the distribution of garage door openers and printer cartridges? I was told today, there was an injunction issued this morning in the printer cartridge case, the Lexmark case against the company that was distributing substitute printer cartridges because it read a bit of code on the header file, or inside the printer, that enabled them to substitute. Now, I would say this is out of the scope of the DMCA. It was not what we intended when we were drafting the provisions of the DMCA. I think that we need to come back to reality because we do not want to live in a society where, by putting five bits of code in front of any product, you are not allowed to, and you are committing a crime if you use that product. This is a travesty, and this needs to be addressed legislatively because the law here is not at all clear.

The last thing I am going to talk about is the Broadcast Flag. We have a modest proposal on the flag. I think that, in the interest of what Mr. Farber said, and I take him seriously, we have to stop with the religious objection to something just because it's proposed from one side or the other. We really have to try to listen to what they are trying to effect. The point of the Broadcast Flag is that it is a very limited technology. The way it is proposed today, you can make unlimited physical copies of television programs if that's your desire. You can also circulate it within a home network. I think if we religiously oppose the Broadcast Flag as an industry, we are going to be sending the message to the entertainment industry that we're not willing to cooperate on anything. And that is going to lead to a Hollings-type approach, which I think we can all agree is anathema and is going to retard innovation in our industry for years and years to come.

We do have questions about how a Broadcast Flag would be implemented. We would prefer that the FCC not take jurisdiction over this because we think it is the thin edge of a wedge for government to start regulating the network. But if we don't listen to the concerns of copyright owners and effect reasonable rules for distribution of content within a home network, then we're not doing our part as an industry.

So, there are challenges for all of us, but DRM is here today, in the marketplace. DRM is an abstract concept. It's just a set of technologies. It can be used for good or for ill, and as always, the challenge is to craft the balance that will enable us to move forward. Thanks.

GREEN: I would like to make one comment to Alex's statement regarding Lexmark. I think most consumers and most rational, reasonable people probably would agree that the uses to which the DMCA has been

put by the industry were not within the scope at the time the legislature passed this law. However, everybody, certainly those pushing DRM onto the consumer, will all readily agree that DMCA has been overused, and some of these uses of it have really been an abuse—for example, we had the printer cartridge, and another one that you may not be aware of, which hasn't been litigated yet, is the cell phone batteries in your phone, which not only do cell phones not accept some third, some after-market batteries, but the ones you are getting from your vendor in many cases have secure chips in them that keep track of how many times the battery has been re-charged, and as this counter goes up, the battery will accept less and less charge, not because the battery's running out but because the chip counter tells it to accept less charge so you have to buy a new one.

. . . .

It really does not matter what the proponents and providers of DRM believe that DRM should be placed to. All that matters is what the courts believe, and the courts believe that these uses of DRM and the DMCA are legitimate. I would like to echo what Alex said. Unless the law is changed, these abuses are not unlikely to diminish, but only likely to increase. So let's be careful with what we're asking for.

. . . .

QUESTIONER, PAM SAMUELSON, BOALT HALL: I would like the panelist to talk a little bit about patents on DRM technology. It's my understanding that there are two seemingly conflicting patents, one owned by InterTrust and one owned by ContentGuard, and it seems to me that when we're talking about competition and innovation, if you have two—the InterTrust patent, as I understand it, has recently been acquired by, I think, Sony and Philips—big players, how does an open source developer who might want to do DRM do so, or where does the individual author turn, who might want to self publish and use a DRM system, but finds him or herself in a marketplace where only the big players are licensed to use these patents? It seems to me that there are some interesting issues, and I'd just like to see what, if any, comments you might have about that.

FARBER: There are more than just those two in the rights management patent game, and there's going to be some interesting battles on those. That's a big problem. A lot of those patents, in my humble opinion, aren't worth the paper they're written on, but that doesn't prove very much in the courts. My main observation is it's more than two. There are a number that have patents that are put in this area, and a lot of old technology that I think is prior art.

MANFERDELLI: I would say so; the InterTrust one, we're the one being sued, so I'm not going to say a word about that. I know that much. I don't think ContentGuard is in any litigation at all. I do think that whatever the terms of use are quite important. I think, you know, there are several levels of use. There'll be many vendors selling DRM systems, and my expectation is that after the mess quiets down, they'll be licensed one way or another. And the publisher, whoever is trying to publish the content, whatever it is, will most likely use one of them under reasonable terms, but it's got to settle down first. I'm not sure what else to say since I can't tell you what the patents are going to cost under certain circumstances, and as I said, in the particular circumstance you brought up, I don't control that. Microsoft does own a part of ContentGuard, but it's a minority share. Patents are a difficult issue, period. You could probably have several conferences on that without a complete resolution of the details. And I don't know what else to say, except we, in technology, not DRM, who live in that patent environment, we're just going to have to muddle through for a while.

. . . .

GREEN: Certainly patents by their very nature are intended to prevent competitors from producing products that will compete with the offerings that you are making. If a company chooses to not license a patent that's underlying some dear and near technology, and thus, prevents, for example, open source competitors, for whom it is very difficult to license patents on anything other than a world-wide, royalty-free basis, I would contend that the not licensing, and thus preventing the open-source competitor from entering a market, is not necessarily incompatible with the business models of the patent holders.

One patent that springs to mind here, that actually I haven't heard much about, and maybe John [Manferdelli] can enlighten us here, the new DRM technology, formerly called Palladium, now an acronym nobody can pronounce—Next Generation Secure Computing Base—is based on a patent that Microsoft holds called the Digital Rights Management Operating System patent. In the past, and certainly in the present, Microsoft has frequently stated that one could build an open source implementation on top of the underlying technologies, build their own secure micro-kernel on a technology on which Microsoft holds the patent, as an open source application. What I haven't seen so far is a public statement by Microsoft that Microsoft intends to license this patent world-wide on an open source development, on a royalty-free, in perpetual, basis. Is that Microsoft's intent?

MANFERDELLI: Let me first say, the technology, whose name I'm not going to try to re-pronounce, is not based solely on that patent. We'd

probably name it differently than we did for that patent, not just because it would have sounded better, but because what we're thinking of doing with it is a bit different.

You're right, though; Microsoft has not announced any patent licensing policy on that particular patent. I can't tell you anything other than I hope we do soon.

III. IMPACTS OF DRMS ON FLOWS OF INFORMATION

Panel:

David Wagner, Computer Science, University of California, Berkeley (moderator)

Hal Abelson, Massachusetts Institute of Technology

John Erickson, Hewlett-Packard Co.

Joseph Liu, Boston College Law School

Edward Felten, Computer Science, Princeton University

Larry Lessig, Stanford Law School

WAGNER: We've got a great session for you here. My name is Dave Wagner, I'm from the computer science department here at Berkeley and we're going to be talking about the impact of digital rights management on information flows. We've got a fantastic lineup of speakers today. So let me introduce you to our panelists. I'll introduce them in the order they are going to speak. I've asked them each to speak for ten minutes on the topic, and we should get a nice diverse set of perspectives.

At the far end, Hal Abelson will kick us off. Hal is a professor of computer science at MIT. His name is familiar to me as a computer scientist because he is one of the co-authors of one of the classic introductory textbooks of computer science. He is also a long-standing member of the computer science committee. He's done some great work. He's widely recognized for his teaching and other efforts. Second speaking will be John Erickson, who is a principal scientist at HP Labs. He tells me he's been doing work on digital rights management since before it was called DRM. It's great to have industry's perspective. Third we have Joe Liu from Boston College Law School, where he is a professor. He has a paper in the proceedings addressing the impact of DMCA on researchers and on scientific research, which I highly recommend to you. And then Ed Felten will be speaking fourth. Ed is a professor of computer science at Princeton University. You may know Ed—Ed is famous for many reasons. He served as an expert witness in the Microsoft trial. He's been threatened

with a lawsuit because of a paper he wanted to publish. But I can tell you as a fellow computer scientist, he has also done fantastic research in computer security and related fields. I suspect he's become more of an expert on the DMCA than he expected to be, and he's going to give us a perspective on some of the public policy impacts of the laws. Then finally Larry Lessig will speak. Larry is a professor of law at Stanford University and has written a number of seminal books in the field, and is the chairman of the Creative Commons project. He'll be speaking about the Creative Commons. So without any further ado let me just hand things off to Hal, who will get things started.

ABELSON: I couldn't help putting up this nice picture of the Statute of Anne where supposedly all of this recognition of the rights of the creators comes from. Pam [Samuelson] also said that of the communities that are here, she'd like us to talk to the policy makers, so what I want to say to the policy makers is: watch out. You are surrounded here by two very dangerous, delusional communities: the lawyers and the computer scientists, who tend to suffer from the same delusion, and that delusion is that you make things better by making them more precise. So let's take a reminder of what it is we're trying to do. See, there's this thing called the public good, and then the lawyers go and create laws about the public good, and already you see the legal code—Larry [Lessig]'s word—is at best a fuzzy reflection of this thing called the public good. Then the computer scientists get into the act and they create these things called standards, which supposedly implement some impression of what the law is. And while it's actually pretty bad, it's hard to make a DRM standard that has fair use, so let's sort of not worry about that now—maybe we'll get one in ten years and then the real joke happens. The computer guys really get into the game, and they make supposed implementations of these standards, which are the biggest distortion of all. Ed made a very good career pointing out the difference between java implementations and java standards as it comes to security, and this is ok, right? This is how the world is. It is not perfect; you're not going to get that last precision of law that reflects public good, you're not going to get that last precision of implementation that reflects standards; and the real problem is, now we come in and we put on this thing, the mattress tag, "do not remove under penalty of law." So let me say to the policy holders as you listen to these things about DRM, the key legal principle that is missing from this discussion is not fair use. That's a lawyer thing, and we've been talking about it the whole time.

The key legal principal missing is the de minimis principle. When we design, when you look at these DRM designs and you evaluate them, you

say, "Have you fallen into the delusions of the computer scientists and the lawyers?", which is often expressed as, "Boy, it would be really great if we put up a system where practice has to conform to policy." It doesn't work that way. We have to look for the friction, the flexibility, the fuzz in these systems that avoids them from being these legal-computer science wet dreams, that if we can only be very precise about everything, that will serve the pubic good. That's not really what I want to talk about. I wanted to selfishly tell you a little bit about my world and what copyright looks like there. This is all about copyright, where we're putting all these systems in, and I wanted to tell you what scientific publishing looks like from the perspective of the research universities.

So the lawyers tell us that this is about the world of scientific journals the lawyers tell us that copyright is policy. So inventors, authors, scientists, are now invited to give their property away to the journals. Give it for free, or in some cases even pay journals to take it by paying page charges. The journals in turn now own this property and all rights to it forever. Well, limited time forever, but forever. And the journals, in some arbitrary scheme that's totally up to them, magnanimously give rights back to the authors. The university actually doesn't enter into this deal at all, and who knows about the public.

So I just wanted to show you for fun some of these contracts by which authors give rights to journals. Here's my association, the ACM (Association for Computing Machinery. I give the ACM the property. It is now their property, and in their generosity, they allow me to post that for my own personal use on a website. But of course, my profession is pretty liberal here. We could look at a more standard thing like Elsevier, we're going to give Elsevier our property and Elsevier is going to give me the right to present my paper at a conference. Isn't that great? Actually, Elsevier's not the worst either. I'm really glad I'm not a chemist. If I were a member of the American Chemical Society, I would have the right to send the paper to fifty of my colleagues and to post not the paper, but the title and the abstract and the figures from it; and of course, all these guys are amateurs if we go look at the New England Journal of Medicine. The New England Journal of Medicine is not confused at all. They said, "This is ours, period. What we give you is, well, you get the same fair use rights that we have to give to everybody else."

Now, why are we making this deal? We're making this deal because publishing is a serious business. This thing is either under the control of the journals or unknown individuals, and "we should not cede copyright to the individual authors." Where did these guys get the copyright from in the first place? So this is not the world that the Statute of Anne ushered in.

This is the world that the Statute of Anne helped usher out, which is the world of the stationer's company. It's the stationers' fall in the early 17th century, and what that world is about. It is not about the creativity of the individual authors. It is about the right going to responsible parties who will exert sort of cartel control because they control the infrastructure. Now is that a good idea? Well sure, publishing is a serious business, and we want all the great things that journals give us, but there's all sorts of other stuff that we might want. We might want indexing. We might want integration into semantic web. We might want all sorts of things that nobody has thought of yet. This is the promise of the Internet.

We put up Google and there's all this wonderful stuff. Unfortunately, it's not the most wonderful stuff because the most wonderful stuff is locked up behind some publisher's wall. What kind of applications can we imagine? Well here's a nice one: it turns out you can go on the web and look at a concordance of the works of Henry James. So I might want to go look at the concordance of *The Turn of the Screw*, which you remember is this wonderful novel about evil. So you might want to see how many times "evil" appears in *Turn of the Screw* and you hit this button. It turns out to be only seven; and then I can look at any one of these places, and I can see the context of where the word "evil" appeared. High school term paper heaven. And I can get that from Henry James and I can get that for Henry Way. I can get that for all sorts of things. No one, of course, after 1923, because the innovation has been stopped. So, the thing I want to leave you with is: Will the need for sophisticated access tools be stillborn? Or, there's actually a flip-side, and the flip-side is that lots of people in this new stationer's company will make lots of investments for this, but what they're going to create are network effects. And these network effects are not about the content. The content, I heard Bob Blakley say, "This is all going to go priced down to zero." This isn't the problem. The problem is that the content infrastructure is going to be owned. If I'm a publisher with a journal which has cross-indexed 50 percent of the literature, why would anybody want to go to another publisher to be a journal? So digital rights management with the force of law behind it can effectively re-create the role of the stationer's company. And I'm not kidding. Here's a quote from a publisher, and this is a marvelously paternalistic quote: "We're going to give scientists all the data they need, universities are going to license it, and we're in charge and you should be happy." Probably half the people in the room can guess who that is. That's Elsevier. Dirk Haank, head of Elsevier should be very happy because Elsevier Science runs at the 37 percent profit margin, and their cost to the libraries has increased at a nine percent annual rate since 1991. The question is: Are we headed back to the

world where we have legally sanctioned monopolies that dominate the infrastructure? The question we should be asking is: Is that world going to be ushered in and cemented for a very, very long time by this approach of digital rights that we're taking? Okay, thank you.

ERICKSON: What I wanted to focus on was the very beginning of what Hal was talking about when he had those overlapping bits and pieces getting fuzzy. I was sort of troubled in what I should call this, whether I should call it "policy enforcement and the free flow of information" or "policy enforcement versus the free flow of information". I think that ultimately, because it's a cautionary note, it needs to be called "versus." I wanted to give some thanks to Larry as well for this notion of "code" being de facto law. The kind of policies I am talking about, fundamentally, are those that are expressed separately. Actually policies are code. They are just separate code, separately managed. The "good parts" version of this story is that we are seeing regimes come out where they are not being built in. We have had generations of policies built with code, bits that are set or not set in digital stream, or simply formats, whether they are analog formats or digital formats, that are used and controlled. By having separately expressed policies, they can be separately managed, they can be dynamically modified. Policies are used wherever a system has to make a choice, and DRM systems are obviously just a subset of that whole world. We are seeing also this emergence of trusted systems, trusted computing bases, platforms or stacks where policies can be enforced in reliable and deterministic ways. As more research is done in the expression of policies and the applications of policies, we see potentially better ways to have policies apply to exact contexts of use.

So the upside is that, this concept of policy enforcement where policies are declaratively expressed, where policies are managed separately from applications, they are yanked out of the hard coded platform, or yanked out of the code, separately managed and applied where they can be studied, analyzed, improved, dynamically changed based upon context, where they can be transparent to what they do and also where the applications that apply them can be transparent, these are all good things. There is a potential to do things in a lot better ways than how they have been done. The scary and nasty bit is that where of course there is still "code." We are limited by the way that the languages themselves are designed, their expressivity. We are limited by the choices that the people make when they write those policies, what they put in, what they leave out. We are limited by the ability of that thing which is going to make that choice, about "what policy do I apply?", of making that right decision. We are limited by that end system which is supposed to apply that, having that capability to actu-

ally do that, regardless of what the policy actually says. We are also limited by the ability, even the scalability of systems, to determine whether or not they trust some other subcomponent which they may have to interact with.

Another way to state a lot of our concerns is policy enforcement regimes allow a sort of private law to be created because, let's face it, they are in fact detached from reality. They are what the implementers decide them to be. As I said in a previous slide, it's what's encoded, what can be encoded, the decisions that people make. There's no governance into what goes into it, there's no social governance into what goes into a rights expression language, for example. But there are other examples: privacy management languages. One exception might be health care, controlling health care information. But you can aspire to have these constitutionally inspired values in these things. I would say that as we look forward into these regimes, if we are to have these regimes, and I think it's a given that we are going to see these things increasingly, we have got to figure out how to include people in the loop. If you count on policy enforcement regimes, DRM systems, to make the right decisions without people as part of the loop, without people being encoded into the loop, without people being able to make their own decisions about whether they will themselves accept liability if, for example, text is exported from a secure format for them to use in like a review, then we have got a problem. So we have to figure out as we establish policy enforcement regimes how to have escapes.

Another problem that is semi-related to this is that DRM systems can make information opaque. DRM systems don't have a monopoly on this. Lots of digital formats make information opaque—you can't see into it. We've got to think of the ways that encourage the rules that enable enhanced usage of the information, but doesn't constrain the flow. We see here that metadata regimes that augment the deployment of information in various formats are absolutely essential. You don't have to look inside that opaque container, even if it's locked up. If you have got appropriate metadata regimes, you can find the right stuff; find out what you need, even if it is in a secure format. But you've got to have both the accessibility of formats and rules that allow you to use that stuff in appropriate ways. There's this notion of closed information spaces which are defined by built-in policies, the formats that are used, the policies that are written. Examples of these include communities that don't work with certain browsers. They break. That's a policy decision, even though it may seem to be a technology decision. Somebody decided that they were going to exclude a particular browser. Also, information control, the use of proprie-

tary media formats, all these sorts of things. So finally how do we—this is borrowing from Larry—how do we challenge the code? How do we hook reality into these systems? How do we write policies and apply policies in a way that both can be processed in an automated and humanistic way? Thank you.

LIU: My brief remarks today are going to focus on a paper that I've written for this conference. The topic of the paper is the impact of the DMCA on academic encryption research. First some background. As you all know Congress enacted the DMCA in 1998, as a response to perceived challenges presented by digital technology. There are provisions in the DMCA, which are the ones we have been talking about, that impose liability for acts of circumvention, and also impose liability for distributing technologies that facilitate circumvention. Now again, all of you know there has been a lot of debate over the wisdom of these provisions. They are very controversial, and in fact, a lot of the discussion in both today's panels and tomorrow's panels will deal with this larger issue, whether this represents a sensible response to digital technology. My paper takes a much narrower focus, and really looks at how this statute impacts a specific group of individuals, namely encryption researchers—even a subset of this group, namely academic encryption researchers. This group is really a group that pretty much everyone agrees should be largely untouched by the DMCA. Even people on the content side, people in Congress and people who oppose the DMCA, have all at least said that this group should be largely unaffected by the DMCA. So what I want to do here is take a look at that, and see exactly to what extent they are untouched by the DMCA.

When Congress was first considering the DMCA, there wasn't any exemption originally for encryption research, and so encryption researchers testified before Congress, explaining that this was problematic because it could impose liability on them for certain activities that they routinely undertake when they are conducting this research. So in response, Congress enacted 1201(g), which is the Encryption Research Exemption and basically exempts good faith encryption research. That of course wasn't the end of the story, because a lot of encryption researchers subsequently objected that this exemption was a bit too narrow to really be of any good, even after the DMCA was enacted. In fact there have been a number of cases since the enactment of the DMCA where researchers have been threatened with suit. The most famous example would be the case of Ed Felten and his group of researchers who cracked the SDMI watermarking technology, and then were subsequently threatened with a possible lawsuit under the DMCA. You have these concerns that this exemption isn't doing

what it's supposed to be doing, and at the same time, other commentators basically suggesting that a lot of these fears are overblown, that in fact if you look at the exemption carefully, researchers really shouldn't be that worried and shouldn't fear liability to any real extent.

The paper itself essentially makes two claims: one a descriptive claim and one a normative claim. The first descriptive claim has two parts: in the paper I basically argue that academic encryption researchers should still be able to conduct some research without significant fear of liability under the DMCA, but the DMCA will have a non-trivial impact on the conditions under which this research takes place. Taking the first half of this descriptive claim, the argument is that if you look at the statute and the legislative history, and you try to anticipate how courts are going to interpret the exemption for some academic encryption researchers, there should be some area within which they should be able to conduct and publish their research without significant fear of liability. The details are in the paper, and I will refer you to the paper itself, but I think this is an important point to note, simply because I think there is a danger when faced with a new statute, and one that hasn't really been interpreted, to see so many flaws in the statute that you really wind up censoring yourself more than you really need to.

That really isn't the end of the story because the DMCA still, even for these folks who might fall within this category, will have a pretty significant impact on how the research is being conducted. This is because the exemption itself isn't a categorical exemption; it's phrased in a way that actually puts a lot of conditions on people who want to take advantage of it. What are those conditions and what sort of effects can we expect the DMCA to have on people who engage in this kind of research? Here are some of them, and these are based again both on a reading of the statute, and also actual cases involving encryption researchers that want to publish their work and are dealing with the DMCA. I am pretty much going to list these rather than going into them in much detail, in the interest of saving time. First, the DMCA is going to have an impact on limiting who can actually conduct this kind of research, and that's because the DMCA itself, if you look at the exemption, gives a preference to folks who have a formal training in this area or are affiliated with a research institution, or some other institution like that. This is despite the fact that a lot of research in this area is done by people who may not have that sort of affiliation. Second, it's going to impose additional hurdles that researchers have to go through before they can engage in this kind of research. Initially, because you need to probably consult a lawyer to make sure that what you're doing falls within the exemption; and secondly, one of the requirements of the

exemption is that a researcher must seek permission from the copyright owner before engaging in an act of circumvention. The statute doesn't actually say that you have to get permission, just that you have to seek it. Third, it will very likely have the effect of limiting free communication about the results of your research. Fourth, it may also limit the avenues for publicizing your research. Again, this is because the statute gives preference to folk who publish in a manner that, generally paraphrasing, encourages the advancement of knowledge in this area, as opposed to facilitating infringement.

Finally, you can expect the DMCA to have an impact on the actual content of the published work itself; and this results from at least two things. First, to the extent that your paper contains actual code, or very specific descriptions about how to circumvent a technology, it begins to look more like a technology or tool that others can use. Second, because the whole structure of this exemption gives notice to copyright owners during the research process, and actually involves them in the process a little bit earlier, you can expect copyright owners then to ask for changes in the paper, changes that might be very hard to resist. So at the end of the day, I'm saying that even though some research can still take place, the conditions under which this research is going to take place are going to be heavily regulated.

Now, how should we think about this impact? The fact that there is an impact on this research may not be the end of the story, because I suppose you could argue that these burdens are a reasonable burden that these researchers should bear in order to have some additional benefits. Well, on the normative front, this paper argues that this impact is in fact extremely problematic and something that we should be troubled about. I think the easiest way to see this is to sort of back up and consider just how far away we are from copyright infringement. In this specific context, the DMCA is having an impact not on copyright infringement, or even the devices that can be used to commit copyright infringement, but here we're regulating basic research that can be used to create devices that can be used to commit copyright infringement. So we're really quite a long distance away from copyright infringement; and when regulating activity this far upstream, I think you need to be really careful about the potential downstream impacts, because potentially there may be all sorts of downstream effects that are unrelated to the problem that this is trying to get at, which is namely copyright infringement. That's really sort of the main message in this paper, and the argument at the end of the day is that the DMCA itself really is not sufficiently careful about these downstream impacts. That in trying to get at copyright infringement, it really is having this impact in

this specific area, on some collateral area that really is quite unrelated, or can be unrelated, to copyright infringement. Thank you.

FELTEN: I'd like to talk about the interaction between DRM and public policy, but I'm not going to come at that from the ordinary direction, saying what public policy should be about DRM. I want to talk instead about what the impact of DRM is on the public policy process related to other issues. That is, my argument will be that DRM not only is a public policy issue itself, but that it has a negative impact on the public policy debate.

Basically this stems from the fact that DRM strategies tend to take devices, whether they are computers or media players, and turn them into black boxes, black boxes that users are not supposed to, or allowed to, analyze or examine or understand. This goes under a lot of different euphemistic names. Sometimes it's called a secure execution environment, sometimes people say that the device is an appliance, although that's also a misnomer. It's not like any normal appliance you might have in your house. Sometimes it's called the robustness requirement. But all of these things really mean that the technology is supposed to be a black box, you're not supposed to be able to look inside of it. And this black box effect tends to grow over the scope of the system. For example, if you're talking about a computer system, you might say, "Well, only the part that deals with the media has to be a black box." The boundaries of that black box tend to grow because there's concern that the content will be grabbed off of the video card or the audio card, that it would be grabbed off of the disk, that it will be grabbed as it goes across the system's IO bus, and so on. The result is that the entire device tends to get turned into a black box. There's a combination of technology and law that's used to try and make these devices into black boxes. The devices are engineered in a way that armors them so that it's difficult technically to analyze or understand what's happening inside the device.

The use of a particular kind of black box design may be mandated by law—that's essentially what the tech mandates in the Hollings bill would do—and possibly, the black box nature of the systems is backed by laws like the DMCA that tend to ban analysis or tinkering or discussion related to the device. So as a result of all of this, DRM and the things that come with DRM turn technological devices into black boxes.

Now, the other side of this has to do with the interaction between technology and public policy. There are a lot of important policy questions that depend in an intimate way on understanding technology, and understanding of the technology: an important input to making reasonable public policy decisions. This is especially true right now with respect to the

things that are at stake with DRM; and so I'm going to argue that bans on understanding technology tend to cripple the public debate about these issues.

Now there are lots of examples of issues in which this is true and I want to give you three examples, but just to raise the degree of difficulty a little bit and hopefully help convince you that there are many, many examples, I'm going to use what other people have already mentioned in the conference. The first one was mentioned by Dave Farber this morning, the Total Information Awareness Program. This is obviously a public policy issue that's very much at the forefront now. I managed to get a copy of their logo off another website instead of taking it down. The logo's not too popular. I imagine the name Total Information Awareness is likely to get changed to something like Next Generation Secure Information Awareness. So here's the public policy issue with TIA. Law enforcement and intelligence communities in the United States want to mine commercial databases. They want to do it for good reasons, to catch people who would like to blow us up. But there is a significant privacy issue involved here. The advocates of TIA say that we shouldn't worry too much about abuses by rogue agents, by rogue law enforcement personnel, because methods like DRM, methods designed to prevent misuse of information or violations of policy, will prevent them. Is this true? Well, if you want to know, then you need to understand the black boxes, you need to understand the efficacy of DRM technology, whether it's going to work. You need to be able to take a skeptical look at this technology and understand how much can we count on it. And that's an important factor in any public policy decision that one might make about TIA.

My second example comes from Bob Blakley's talk this morning: the "Girls Gone Wild" video or, in particular, the attempt to block it. Another public policy issue before us has to do with blocking and filtering technology. For example, there are products out there that claim to block pornographic websites, and they claim not to block non-porn content. Is this true? Should we use this technology in schools and libraries and homes and so on? The advocates of this technology claim that we shouldn't worry about over-blocking because their blocking list, the list of sites to block, is accurate. Is that true? If we want to know whether or not it's true, we need to be able to open up their black box and see what their block list actually is. There's a lawsuit brought by Ben Edelman, a researcher at Harvard, about this very issue under the DMCA. We need to look inside that black box in order to understand the accuracy of the block list, and again, that's an important input to the public policy decision that needs to get made.

My third example is an electronic voting machine—all electronic. You walk up to it, you push some buttons on the front, and it records your vote. At the end of the election, it spits up a count of how many votes were cast for each candidate, or at least we hope it does that. So after the Florida 2000 election, there was a big push toward different voting technology, in particular computerized voting machines. Counties all over the place are looking at that. Santa Clara County, California, is in the middle of a decision process, and my own county, Mercer County, in New Jersey, is also in the throes of a decision about whether to go ahead with computerized voting, or what kind of computerized voting. You face a lot of tradeoffs there. There's no doubt that direct-recording electronic, the all electronic machines, are convenient to use and at the end of the election you get a count really fast. The big problem, though, is the risk of fraud. How do you know that the election result is right? How do you know that there hasn't been some sort of horrible mistake? Of course, this is a problem that has gone back a long time in elections, but we change it when we move to an electronic system. We change the kind of failure modes that we face. The advocates of these technologies, mostly the vendors, say, "Don't worry about tampering. We use methods to seal the devices so that outsiders can't tamper, people at the polling place can't tamper with it." They claim to use methods that prevent even their own engineers from changing what the machines do. Is that true? Do the technologies they use actually prevent tampering? How difficult is it to tamper? Is it even possible to do that? We need to understand the black boxes that they're building, and we need to understand black box technologies in general, to be able to evaluate that.

In all three of these cases, all three of the policy examples, we need to answer basic technological questions about black boxes in general, and specific black boxes, in order to make good public policy decisions. Given more time, I could go on and on and talk about other examples. There are lots of examples related to technology policy, to regulation of spectrum and examples related to defense, and so on. I'll just point out that in my view this is a serious problem. People don't understand enough about technology. Technology, God knows, is hard enough to figure out. What we don't need to do is make it harder. Thank you.

LESSIG: Excellent. So, we've been talking about DRM forever. Forever. For as long as I can remember, and that's forever for me. So forever we've been struggling with this issue of "How are we going to confront the world where not only rights existed, and were expressed strongly, but technology enabled people to enforce rights strongly?" And after struggling with this forever, I'm increasingly convinced that we've got to re-

frame this problem because a lot of bright people have tried to figure out the answer to this problem, both on their side and our side, and none of us have a good clue yet about how to solve this problem. So, re-frame the problem.

There are basically three kinds of people out there. Usually there are two, but I found out there were three. There are three kinds of people out there. There are basically people out there who believe in not controlling their stuff at all. We call them communists, you know, but there are people that say, "Take my stuff and do with it what you want." Then there are people out there who say, "Don't touch my stuff unless you ask my permission. Don't do anything with it at all unless you've got some affirmative rights from me." And then there's the rest of us in the middle who say, "Go ahead use it for lots of obvious reasons. Of course, don't make a Disney movie out of it, but for most reasons we're completely happy that you take and use my stuff." There are, therefore, the "none," none of my rights respected, and the "alls," I want all of my rights respected, and the "somes," I want some of my rights respected.

Now in the beginning, the beginning of the Internet, we had an architecture that essentially ratified the position of the "nones," the people who said, "I don't want to control my stuff at all." We had a technology that enabled basically everybody to take everything that's out there, and to share everything, and to share it in the most extraordinary efficient way, and that was great. But, that created a lot of complaints, obviously from the people who are at least in the "all" category, because their fear was that this architecture of the "nones" would increasingly shrink the space that the "alls" could adopt. Also, those out there putting stuff up in the "some" category, too, would have their rights shrunk if none of the rights that might be respected here would have been respected under the architecture of the "none."

So that was where we were, and the problem from that perspective was that there was an obvious political response: Those with all the money are also those with all the rights and those that want to assert the rights, and they would force on this world a shift in this architecture. They would try to flip the default away from a default that supported the "none" to a default that supported the "all." So in the future, increasingly, they promise us an architecture which is the DRM architecture that takes this world where there are three categories and flips it from the default where "none" control to the default where "all" is the rule—where all rights being controlled is the normal way in which we engage in interactions with each other, and the consequence of that is the exact same consequence we've seen before, but now flipped. It becomes harder and harder for the

"somes" to actually be out there, and express themselves in a way that says, "Here, take and share and use," because they must embody and adopt these highly expensive and burdensome technologies to say, "Do with my stuff as you wish so long as you respect the following rights." And also, it criminalizes the category of the "nones" out there, criminal "nones" running around, who are increasingly pushed off this space so that the default world of total control supported by total information awareness makes it possible for the "alls" to control—you got it—everything.

Now here's the problem. We've been solving for the extremes here. We've been thinking about the world as if there's either those who care not at all or those who care in the extreme; and the problem with that solution on either side is that it defeats the massive and most important category of people in the middle, who would actually like a way to express the view that you should be able to take and share the content without suffering the deep burdens of DRM. So what we need here is a way to recognize this middle. Now, there are two strategies that have been adopted to attempt to recognize this middle. The first strategy is the one we're familiar with because a lot of us have been fighting it, maybe all of us have been fighting it, on one side or the other. We've been fighting it in the courts and Congress to get them to say, "Regulate this world in a way so that the potential for the 'all' to control everything is balanced. Restrict DRM in the following ways so that we can at least have fair use or ensure that the DRM technologies that go out there don't displace the possibility of free content to be distributed."

That's a strategy. But increasingly I'm becoming convinced that that's not a strategy that is going to work in time. And that forces, I think, us to consider a second strategy, which is increasingly the one I think we ought to be spending our time on. Instead of ways to fight or limit DRM, what we need is a strategy that expresses this middle space. So I and Hal and other people in this audience are part of an organization called the Creative Commons. The Creative Commons believes that we need to distinguish between this idea, DRM, and this idea, DRE. We have to understand that there are two separate issues here, and we shouldn't be solving them together, at least not now. We ought to be finding a way for people to express, simply and easily, "Here is the set of rights that I'm happy that you respect," without building into that expression the technologies that make it so that those rights are automatically, by machines, enforced. Not because no one should be able to do that—let the "alls" do that, that's fine—but because most of the content out there is not content for which this extraordinarily strong mechanism of control is needed or valuable. The point is, for the green space in the center, these technologies of control are not

just hassles, they defeat the opportunity for this content to be shared freely in a way in which the author plainly wants. So we need a way to express digital rights without that expression forcing them necessarily. A technology to say that this is free, or at least this is sort of free, some rights reserved, not all rights reserved, and that's the role we believe Creative Commons, in its first instantiation, plays.

Creative Commons says, "We are going to build a layer of reasonable copyright law out there on top of this background of unreasonable extremism." We live in a world now governed by this unreasonable extremism, and we can do something about that by expressing a reasonable middle. This is a technology to do it, so that this background of control gets flooded by a default expression that says, "Go ahead a share in a certain way," without attempting to say to the "alls," "You shouldn't be allowed to do what you do," but instead by enabling the rest of the world to create content that is shareable freely, and can compete with those who insist on controlling all of their rights—restoring, then, in this context, reasonableness through voluntary action.

Now why is this important? Well, one story that's been told out there about why the Creative Commons project is important is that it's going to be good for the incentives of certain artists. We have artists who are out there who have begun to say, "Yeah, it's better for me to share my content in this way than to adopt the all rights reserved model." So Cory Doctorow, a hero of mine, published an extraordinary novel, *Down and Out in the Magic Kingdom*. On the same day it's in the bookstores, it's on the web under a CC license; download it, do with it as you wish. He sells an extraordinary number of books in the bookstores; he gives away a massively large number of books on the web, and what he's done, thereby, is increased the exposure of the world to Cory Doctorow's extraordinary writing, and he believes that will make it easier for him to be a successful writer in the future.

I'm all for it. It's exactly what we should be enabling: this creative use of the 'Net in a way that spreads culture broadly. But that's not the important, or most important reason, that people ought to participate in this expression of something different. The most important reason is we ought to begin to identify, to put our hands up around the world in a way that says, "I believe in free here. The default is control, but I believe in free, or I believe in somewhat free, but I believe in it now and urgently because the shift that we've seen has radically transformed the opportunity of this technology, of the Internet, to be used to develop something different, some expression in creativity innovation different from the innovation and expression controlled by that tiny little red box in the corner."

Now when this battle began, people said, "If it's either the 'nones' or the 'alls,' the 'alls' are going to win." And when you think about the places where this battle can be fought, I believed we would lose if all we had to do was fight it in the context of Congress, because the "alls" have it all and they can go to Congress, which responds to the "alls." So they were lobbying away. I was that naive person who believed that there was a place out there that we could argue this, as a matter of ideals and principles, to establish a balance here that I thought the framers of our Constitution already gave us 210 years ago. I was wrong. I was wrong. People said, "They weren't ready." I said, "Yes, they are." I was wrong. They were right.

And the consequence of them being right and me being wrong is that the courts have backed out of this battle just at the time when they could have done the most good by expressing ideals that the best interpretation of our Constitution says our framers already expressed, because our framers recognized what Hal was teaching us about, the ideals behind the Statute of Anne. When I lost and we lost, a very kind lobbyist from the other side called me and he said, "You know Larry, look, all you had was ideals and principles on your side." They had, or "We had," he said, "all the money in the world." And he said to me, "When was the last time ideals and principles won over all the money in the world." I thought, "My God, racism, we were just fighting a bunch of racists, right?" The 14th Amendment was about the ideals of the civil rights movement, it wasn't all the money in the world. Here and now, the question we ought to ask is not "When's the last time?" but "When's the next time?"—"When's the next time that ideals and principles win over all the money in the world?" And the next time it does is the time when we, all of us, begin to express in our every step, an expression that says we believe in something different, that we believe in this reasonableness, not the extremism, and we show reasonableness by building this balance in the space that marks the place we're most familiar with, this extraordinary space of potential creativity we call the Internet. We can reclaim, through voluntary efforts that say, "We believe in freedom and we show it because our content expresses it," and let them respect what we say. Thank you very much.

. . . .

QUESTIONER, SAMUELSON: So yesterday when I was doing the tutorial, Alex Alben asked me a question which, because I'm not a technologist, I was not in a very good position to try to answer, but there are several technologists on this panel who are interested in information flows. The question that was put to me was a question about whether it was possible to develop technologies that would allow circumvention for

fair use or other non-infringing purposes. Is it possible to sort of think creatively about anticircumvention laws that might allow some room for circumvention for fair uses without opening up the Pandora's box so that allowing these technologies means that you've essentially repealed the anti-circumvention laws?

ERICKSON: Yes and No. Well, I think that you can try to approximate and perhaps reach a reasonable compromise in how you write the rules that control how the systems operate. So that's one approach. Depending on how far you carry the discussions that lead to that compromise, and, I would argue, how you would include people in the loop so that it's not a completely automated thing, you might be able to do some things. I don't want to talk to the other questions about the increasing of circumvention devices to do the fair use piece, but the one particular piece that I'd like to offer up as a "maybe" or a "yes" is the creation of good policy that includes people.

FELTEN: I think this is one of the most important technical questions surrounding DRM: whether we know, whether we can figure out how to accommodate fair use and other lawful use without opening up a big loophole. The answer, I think, right now, is that we don't know how to do that. Not effectively. A lot of people would like to know whether we can do that, or how we go about doing it, but it's a big open question right now.

ABELSON: I'll give you a little piece of an idea I wouldn't necessarily advocate. This was a little system that was designed by a couple of students in a class I taught in the fall where the notion is that you did this digital rights decision based on some combination of what's carried with the work and something that's asserted by the user, partly who they are and what their intent is. So you get something that sort of gives you increased extra access to this work. On the other hand, either you have some way of saying something about yourself or some way of testing the thing that goes into some record. I don't actually think this is a workable solution, but it's the beginning of an idea.

LIU: I will say something about the legal side of things. I don't know very much about the technical question, and technologically whether this is feasible; but on the legal side, in hearing about this debate, about whether we can effectuate fair use in some sort of technical way, I sort of thought about a thought experiment of what would fair use look like if we tried to implement it in terms of a legal regulatory framework. If we actually tried to spell out, in the law, in a detailed manner, instead of the four factors, what exactly copyright and fair use would look like, I think you would soon find a statute that would begin to resemble the tax code in its complexity because it would be volumes and volumes and volumes of

very detailed regulations depending on who you are, why you're using it, which context, and all the rest. So I think, in sort of referring back to Hal's very initial picture, that first layer that's put on the public interest, I think itself is really subject to a lot of these issues. That's entirely understandable because people's interaction with information is a very complex thing, and I think that it's just really hard to specify, even from a legal standpoint.

QUESTIONER, LEMLEY: This is a question for Larry Lessig primarily. So five years ago at this conference, Bob Gomulkiewicz of Microsoft pointed out a very nice sort of inversion, which is that shrink-wrap licenses and contractual enforcement of big package software on uniform terms also turns out to be the legal basis, to the extent there is one, for the support of the open software movement. One of the interesting things that that pointed out, in a contract sense, was that in order to make a judgment about whether regulation, or freedom from regulation, was the right choice, you had to look not just at what the big guys were going to do, but what the little guys were going to do. I guess I wonder why there isn't a similar kind of dichotomy, and a similar issue that Creative Commons brings forward. It's very easy to write a set of legal rules that says everyone gets a certain set of rights. What you want to do, I take it, is to write a set of legal rules that says everyone gets a different set of rights, they can choose from among an infinite palette. But in order to implement that, it seems to me you need some kind of DRM, or if you want to call it DRE, that's fine. That requires you, though, to take a position about whether regulation of DRM by government is a good thing or a bad thing, right? And I guess what I wonder is whether a group like Creative Commons, that depends, in some sense, on the enabling features of DRM, is also going to facilitate, by allowing DRM, the problems that other people have mentioned at this conference with DRM, not limited by consumer regulation, privacy regulation, whatever else we think is problematic.

LESSIG: So the only part that I want to really resist in the structure of your question is not that it begins with the word 'so.' I did that too. It is the quickness with which you passed over the possible distinction between DRE and DRM. Because I really do think—I didn't think this originally, so I hope this is progress in my thinking—but I really do think that there is a difference between DRE and DRM. And the reason isn't the static difference because, you know, in some sense DRM includes DRE; you've got a digital rights expression language within DRM, and then DRM adds a dollop of control on top of it. That's not the difference. The difference is the dynamic effect it would have on this debate if we had a bunch of content out there that was efficiently expressing the freedom to use it in cer-

tain ways, and a bunch of people out there respecting how it can be used and how it can't be used, and a bunch of people building on that expression of freedom, versus those who continue to insist on this extraordinary overhead of technology that gets built into their content before they share their content. I think those who adopt the DRE side would be in a competitively better position against the DRM crowd in selling and making their content available. They'd be able to say, "I've got better content, not just because it's good content, but because it's freer content," right? So I want to enable that battle because I believe we're in a world where DRM is on the field. I would prefer to be in that world where DRM just wasn't getting on the field, and so if five years ago we could have found some way to keep DRM off the field, then of course we wouldn't be here fighting for Creative Commons, right? There wouldn't be a need for it. But the fact is, if DRM is on the field and is the default, and you allow them to suggest that those of us in the "some" category should just adopt the DRM technology and open up all the permissions. If you allow them to suggest that that's the same, then I think that that world of that technology of control, controlling and taking over more and more of the creative process, is inevitable. And so what I want to do is just break that down. I don't know if it works, I don't know the consequence of it.

LEMLEY: Let me just try one push. That argument makes sense to me. I guess I wonder what the impact is on regulation of DRM technology that might in other circumstances occur for purposes of consumer protection. So Julie Cohen's got a paper that makes the very nice point that DRM is necessarily at odds with strong privacy protection. Isn't DRE also necessarily at odds with strong privacy protection for the same reasons, and don't you find yourself in a position in which, if we move to a DRE world, we're less likely to be regulating privacy protection?

LESSIG: I'd be interested, but I don't think DRE technologies have the same problems that Julie articulates in the "right to anonymity" argument. I don't think it has the same problems. But the other side of this is, this is not a way of saying, "We don't have to worry about the regulations that DRM affects." We've still got to worry about them profoundly, and we've got to worry about DRM technologies restricting fair use. We've got to think creatively about how to carve that back, and so that means pursuing Pam's question and finding a technological answer and figuring out how the law shouldn't be regulated. I'm not saying that these aren't important issues anymore, but I'm saying that it's going to be easier to make those arguments if the other side of the debate is not a picture of a child with forty billion songs on his or her hard disk. It's going to be easier if you can say, "Here's something different from your model of total con-

trol and total anarchy, and one that I don't think runs into a lot of the same problems because, again, remember the DRE here is just enabling a simple way to identify so then I can make a decision about what I want to do with the content." So we want to build on top of the Google API so you can say, "Give me all the pictures of the Empire State Building available for non-commercial use." Bingo. There they are. And now that's content that I can decide to incorporate in my webpage or in my publication that competes with Microsoft's, I mean, sorry, Bill Gate's technology. To have all of this content wrapped in DRM stuff competes with it. So I think that if we had a competition between freed and controlled, freed would win in a large range of cases. Not all. But I still think that it would generally win.

FELTEN: There's an important distinction here between DRE, which gives a way to express the content creators' desires over how something will be used. I think when you talk about rigid enforcement mechanisms, then you raise significant privacy issues. If you just want to give the content creator a way of saying what permissions they grant, then the privacy issues are much easier to deal with.

QUESTIONER, EDDAN KATZ, U.C. BERKELEY: This is a question also for Professor Lessig. In the spirit of avoiding the binary, I'm afraid and troubled by the fact that I leave your talk with, imprinted in my memory, the courts and Congress crossed out in red from when you said, "We asked a question and we lost." I'm wondering if the way the question was posed was the only possible way and if you could think of another way that the question could be posed so that those two channels could further be pursued.

LESSIG: We're lawyers; we can't give up the courts, so we're going to be fighting lots of issues in the courts forever, and the Center for Internet Society at Stanford is fighting. EFF is fighting. We'll continue to fight. The fact is, we lost in the Supreme Court because the average view in the Supreme Court is just like the average view of most Americans about these issues, right? So that means we have a lot of work to do so that most Americans begin to understand how this is a more complicated issue than the binary framing of it. This is the optimism: ordinary people get it when you tell it to them and you explain it to them. They don't have a vested interest in the red "control everything" box, they don't. Ordinary people understand that when we can start thinking about digital creativity, when we can contrast the analog consumer, that's the couch potato, with the digital consumer, that's the person who's taking content, and remixing it, and releasing it in this creative way. The point is, this movement, not because of these lawsuits, but because of what thousands of people have done and lots of them here, is salient out there among ordinary people.

Now, I can shift into pessimism mood really quickly. I won't. Let's just end on the optimistic side. I think if you explain it clearly and repeatedly, over time they will get it; and when they get it, we will win. But it's going to take a lot of work. It was easier to imagine the happiness of five votes than it will be to imagine the battle that is required right now; but, you know, we have no choice. It's got to be that battle right now. I take the only solace from this loss to be the literally thousands of e-mails of people who wrote me and said, "You know, we're going to fight this until we win." That's the solace, and so let's turn that into something productive and optimistic, and I'll be happy to be proven wrong in my pessimism.

IV. DRM-RELATED LEGAL AND POLICY INITIATIVES IN THE UNITED STATES

Panel:

Pam Samuelson, Boalt Hall School of Law, University of California, Berkeley (moderator)

Fritz Attaway, Motion Picture Association of America

Jerry Berman, Center for Democracy and Technology

Ed Black, Computer & Communications Industry Association

Richard Epstein, University of Chicago Law School

Jon Healey, Los Angeles Times

Emery Simon, Business Software Alliance

Mozelle Thompson, Federal Trade Commission

SAMUELSON: This session will be different in format than the other sessions in that each person will not present a paper, but rather it will be a discussion focusing on legal and legislative policy initiatives about DRM in the U.S. So start thinking of your questions. We are going to focus on legal and policy issues related to digital rights. I think it is fair to say that in 1998, when Congress passed the DMCA, they hoped that it had resolved for the foreseeable future the problems or challenges that digital technologies would pose to copyright holders. And they were told, "Just give these few additional rights and everything will be fine." Just five years later, that seems an over-optimistic hope, if there was one. So instead of the thriving e-commerce markets that were anticipated, we have actually a wide array of content available, some of which is freely distrib-

uted, and lawfully so, and some of which is freely distributed, and not so lawfully so.

So Congress and other policy organizations such as the FCC are faced with a number of proposals. Some of those proposals, like the Hollings bill from last year, would have required standard technical measures that would have been embedded in every digital media device. The Broadcast Flag proposal that's now pending before the Federal Communications Commission would strengthen the rights of the rights holders considerably more; and so there are other bills, such as the one Representative Lofgren (D-California) just talked about, and a similar bill that Representative Boucher (D-Virginia) just has already introduced into the 108th Congress, aimed at finding a somewhat greater balance and undoing the excesses of the DMCA. Senator Wyden (D-Oregon) has recently announced that he has some interest in some consumer protection type legislation in relation to labeling DRM-protected material. So I think this Congress will be dealing with consumer protection side issues as well as the content owners' efforts to get stronger and stronger protections.

In addition, I think there have been lawsuits under the DMCA, and also there is a lawsuit brought against one of the recording companies for a defective CD because it caused harm to the computer. That lawsuit just survived a motion to dismiss. So the courts as well as the legislatures are going to be dealing with some consumer protection issues about DRM.

Five years later we know that the DMCA is not being used just to get rid of those black box piracy-enabling technologies, it's being used in a wide variety of other cases like the *Lexmark* case which Representative Lofgren mentioned, as well as the *Chamberlain v. Skylink* case which is about garage door openers. So I think in some sense the DMCA is more controversial now that it was in 1998, and there are calls for an effort to reform the DMCA to get rid of these unintended consequences.

We have with us today a great panel of experts on a wide variety of topics. At the far end of the table is Emery Simon, BSA, and next is Jon Healey, L.A. Times, then Richard Epstein, Fritz Attaway, MPAA, Ed Black, Jerry Berman, Mozelle Thompson, Commissioner of the FTC. The thing to do first is to start with a general question. It seems as though there is a lot of concern over widespread copying. Since this conference is about DRM technology, it seems like a good place to start. Will DRM technology actually solve the piracy problem, mandated or not?

SIMON: Okay, so first of all, let me tell you that I'm in support of the DMCA, and I think it's a good law, not a perfect law, it's got problems, but it's done a lot of good things , but the vilification of the statute astounds me. I work for the software industry. Software piracy costs the

software industry over $11 billion a year. It's not a hypothetical problem, it's a real problem. That piracy steals jobs, tax revenues, steals money for our innovation, The DMCA is a tool. And to see it as an incarnation of a powerful weapon of copyright holders to overreach to extinguish your rights, I think is a little fantastic, in the sense of the reality doesn't match well with that. So to answer your question, piracy is a real problem, and the DMCA is a tool that helps in that fight, and we've had some pretty good litigation to help in that fight. The courts have not had trouble interpreting it, though people may not like those interpretations .

SAMUELSON: If you'll forgive me, that wasn't actually the question I asked, you can say something about that, but the question was not whether the DMCA, but whether DRM, is a solution to the piracy problem.

SIMON: They are a tool in that fight, not a solution, and there will never be a perfect tool, but they are a very powerful and worthwhile tool, absolutely.

EPSTEIN: I think a lot of this depends upon exactly whether you think the tool in this case is sufficient for this task, or whether you think it's overbroad. Going back to the Betamax case, if you stop all contributory infringement, and you stop all use, the question is: Did the legal remedy create a partition between the things you want to stop versus things you don't? And I think the only way to succeed, at least for a part of that task, is to have fairly strong kinds of management rights. To the extent you kill the box, it's taking all kinds of non-infringing uses and subjecting them to similar kinds of restrictions that are imposed on infringing uses. But if you develop a system which in effect will allow owners to charge for digital content, much in the way you charge for telephone use by a per-play basis, then you don't have to worry about improper assignments of digital content, you don't care whether I watch it or someone else watches it. I think the whole point—you know I disagree with Congresswoman Lofgren—is that you really don't want the first-sale doctrine in this kind of a world, but you do want to have the continuous monitoring of this kind of use so that price discrimination can take place. We have to completely rethink the analog world where, if one free copy gets out and is capable of infinite reproduction, then the entire technology is capable of being lost.

ATTAWAY: Well, Emery [Simon]'s answer was the correct answer in my view. DRM is part of the solution, not the entire solution, and the problem we face is uncontrolled trafficking in illicit content over the Internet. DRM technology will help the leakage problem that allows content to get to the Internet in an unprotected form. It will provide us a means to deliver our content to consumers in a secure fashion, but there

will always be leakage. We will have to address that in a couple of ways. One is by increasing security. Second, we have to enforce our rights under the copyright laws. We have to bring actions against mass infringers. We have to use the expedited subpoena rights under the DMCA. I know you probably heard about yesterday with Sarah Deutsch, but in fact a deal was made with the ISPs in 1998, under which they received a broad safe harbor against contributory and vicarious infringement actions, in return for which they agreed to a notice and take down notice, and an expedited subpoena process. Unfortunately some ISPs are trying to renege on that, but at least one district court judge said that they couldn't. The third thing we have to do is to provide consumers with content, in a more convenient and enjoyable form than they can get through illicit methods, and we are trying to do that.

BLACK: Let me just say, first of all, I work for a great cross section of companies that have a great need for, and utilize, IP in many ways, and we are strong supporters of a strong copyright system. But we also, over the years, have understood the value of the balance of that system, and have worked to kind of make sure that we keep a system, which in all ways promotes innovation and keeps competition alive. With regard to the question of DRM, though, in a way, I think it's a little bit the wrong question because, does DRM help solve the problem? Well, the problem is not piracy. The problem is: we are in a different era now. The digital revolution has truly thrust change in innumerable ways, and it requires a rebalancing, a recalibration, a new equilibrium of all the legitimate interests. Hollywood is a legitimate interest. Consumers are a legitimate interest. Libraries, a lot of intervening players—there are a tremendous number of interests here that frankly have been thrown into turmoil because of changes in technology. And the second level changes resulting from that, and what we need to be thinking about, is not solving a piece of the problem, of which too much piracy is part of it, but we need to be rethinking how to restructure our whole information flow restrictions and access issues in a comprehensive way that is fair and is reasonable to most of the players. It's a much bigger issue, and in that context, DRM is a valuable tool and a very dangerous weapon, and it is not easy to define the discussion because there are so many variations of it that are going to be in play.

BERMAN: I'm representing a consumer organization that is very concerned about the Internet and the role of the Internet, as an open communications medium, and an open platform, but I'm just going to answer Pam's question. It is part of the solution, and there will be lots leakage, lots of leakage, but it's part of the package. No one is looking for the perfect solution, but DRM is part of the package, and it's going to be de-

ployed, and consumers and Internet organizations that care about balance within the DRM structure have to pay attention to that deployment.

HEALEY: I don't have opinions, and I'm not speaking for my organization. Just a couple of quick observations: EMusic had been referred to yesterday. They distributed content in a non-DRM format, and their business model was like the major record labels—based on distribution—and they wanted to be paid for their content. When Napster happened, EMusic still had an enforcement tool available to them. They didn't need DRM to go after Napster because essentially, they could use their hash assigned to each of their files. So on the enforcement front, DRM is a tool, but I think from history you can say it's not a necessary tool. On the question of whether EMusic's business model is successful or not, you couldn't conclude that it was successful or not based on whether they had DRM attached or whether the MP3 files are more appealing than DRM files. The question really came down to: what content did they have. That might also involve the DRM issue: because they weren't willing to use DRM, they weren't able to get certain types of content. You have to think very carefully about the relationship between DRM and the business model, because it is not necessarily a given that you have to have it in order to do things like enforcement.

SAMUELSON: The Hollings bill hasn't been reintroduced in this Congress, and it seems unlikely that it will be, but it does seem like the Broadcast Flag issue is a very similar kind of proposal, and so I think it would be good for us to talk about the Broadcast Flag. So Fritz, perhaps you could start us off by telling us why the motion picture industry is so keen on having a Broadcast Flag, and then maybe we can talk about why the BF is not such a great idea.

ATTAWAY: I have to take issue with you. It is not at all a similar proposal to the Hollings bill. It certainly has copyright implications, but at its core, it is a communications issue. Cable and satellite delivery systems, because they have a conditional access system, have the ability to protect content, including preventing content from being redistributed over the Internet. Over-the-air broadcasters do not have the ability, and the question before the FCC is: Should they give off-air broadcasters a level playing field where they can offer program suppliers some security against the redistribution over the Internet? Without that security, content providers will naturally migrate away from off-air broadcast television to cable and satellite. So the issue is maintenance of free television. We support that because free television is a major customer of ours, and we want free television to continue to exist in the marketplace. However if it doesn't, we will market our content through conditional access systems and bypass

free television. I don't think that is in the best interests of consumers, but if one wants to argue, I suppose one can.

BERMAN: I think the Broadcast Flag is certainly not the Hollings bill, and its intent is not. It is in a much narrower field. It's not a bill or a proposal, so it's one size fits all, one technology. But it's very difficult to describe how the flag is going to be deployed, and that's why we have to pay attention to whether it could take on characteristics of the Hollings bill. I think that turns on a number of things. For example, "What kind of process will be available for other technologies to get on both? Table A? Will that be an objective set of criteria? Who will make the decision, the government, or a technology board, or the market, about how you get on that table?" Because it is saying that the government is playing a regulatory role, in terms of putting an imprimatur on technologies. But you have heard the cable people say that they are going to take a standard to the FCC, and also look for a governmental blessing. There is an interesting issue of language. What the Hollings bill was considered was a mandate. When standards bodies involving industry, content and IT agree on a DRM standard which they take to the government, that becomes a standard, not a mandate. The problem has been for consumers, who have not had a clear role in the standards process. It's hard to say it's not a mandate from their point of view if their legitimate concerns have not been taken into account. I think is a serious question: getting the consumer voice into the standards. I'm not saying the Broadcast Flag is wrong, or that it can't be a part solution, but there are serious issues about how it works and whether it's an open process.

SIMON: So the technology companies I work with have been pretty vocal and vehemently opposed to the Hollings bill, and we have a coalition to work hard against it. Is the FCC going to exercise a mandate? The answer is: it's too early to tell because we don't know what the FCC is going to do. The FCC could certainly issue regulations, which would have a pervasive effect on downstream devices, in fact any device that comes into contact with content that originates in the broadcast. In the alternative, the FCC could do very little. So it is simply too early to tell, but the potential is certainly there, for it becoming the kind of mandate that has a pervasive effect that the Hollings bill was intended, or at least conceived, as having.

BLACK: I would agree with the later part of your statement there, that we don't know, but it has aspects of being a mandate. A quick reference to the Hollings bill—I think it was a terrible idea, but a wonderful piece of legislation because it helped galvanize a tremendous amount of interest on this thing. The BF is very complex, and it's hard to separate out the proc-

ess that led up to where we are right now. There are issues of participation, openness, competitiveness, that cloud the concept of a flag. The idea that you could have a flag, in an open container setting world, where you didn't have a mandate from the government a lot of people could say, "Hey, let's try it. See if it has some value." When it starts getting to be a standard chosen by a small group of players, and in the formulation we think it is likely to be involving, which gets into the future leverage over how it will be done, they will be able to change it with no outside involvement, just on their own will, a small group of companies. There are a lot of aspects of this broadcast right proposal that are terribly troubling, and if it, in any version we are seeing, is even close to coming to fruition here, and is in fact supported by the FCC, I think we would have a very bad situation.

THOMPSON: I'm from the government and I'm here to help you. (laughter) At the outset, my general counsel requires me to say that my comments here are my own and not necessarily those of the other commissioners. Listening to what I've heard so far, I hear your questions, Pam, but I'm not sure the questions you ask are the ones you really mean to ask. It's like how we view antitrust and consumer protection. There is nothing wrong with being a monopolist, it depends on how you achieve the monopoly and it depends on how you achieve market power. The same principles are applicable here because what we are talking about is standards setting, whether it's done by a self-regulatory body or whether it's done by the government. The question is: Does the standard actually appear to be overbroad, so instead of protecting innovation and incentiving innovation, it actually casts a chill on innovation, and actually thwarts the very purpose of having intellectual property rights? The question is not: DRM, yes or no? It can be a helpful tool. It's under what context it's being developed and how it's being used. The same thing for the Broadcast Flag legislation too often we hear people talking from the polar extremes. We are not talking the field of dreams: Build it and they will come. We have a lot of people out there who want access to content. What I find very interesting is that we are increasingly a demand- driven economy, where consumer confidence becomes important, but what I see is very little being done to focus on what the demand is, and what are the levers that you can use to create demand. So no one knows exactly what consumers are thinking, or they don't think in the long term. Instead you see proposals, which are kind of like eating your young. "Let's figure out how to make this work against the people we want to attract." I don't think that's a long term winning strategy for anyone.

EPSTEIN: I have a simple question, as someone who is kind of an outside expert to the area. I think the basic thing you want to achieve by this system is to make sure that marked content, which in fact is proprietary and protected, is not subject to unauthorized use. The question I have to ask is whether or not when you do this, you engage in various kinds of restraints, which blocks free entry by other parties. So protecting property rights without creating monopolies is the basic task you are trying to achieve; and until someone tells me enough about the specifics of the legislation, I don't know whether or not we are cartelizing an industry, or whether we are protecting property. Until someone answers that question, I can't tell you whether or not I'm for or against the proposal, and if you are going to try and win the public over, they are not much more educated than I am on this kind of issue, and somebody is going to have to be a little bit more specific. So I can almost answer this with, "How are you going to avoid the monopoly problem while you solve the protection problem?"

ATTAWAY: What monopoly problem do you see? (laughter) We are not in the business of creating the essential material. We make entertainment. Quite frankly, sometimes we make movies we can't subpoena people to see.

THOMPSON: You fly to Washington and tell us how important your industry is, and now you come here and play, like "Oh, we're just fluff ?"

ATTAWAY: Well, just the opposite. We are very successful in creating entertainment that a lot of people want to see. We are successful not only in this country, but around the world, in creating content that people want to see. But copyright has been described as a monopoly. It is an exclusive right to maintain control of that creative content, and that is not a bad thing, it's a good thing, because it incentivizes the creation and distribution of that content, which is what the Supreme Court just said in the *Eldred* case. That was a ringing endorsement of the monopoly of copyright. It is a good thing, it's not a bad thing.

EPSTEIN: Well, monopoly could mean one of two things: it could mean the protection of an individual work, or it could mean the cartelizing of an industry. It's the same problem as you have on the patent side. If it's just the former, I'm with you. But if it's the second, I'm against you. As far as *Eldred*, it was one of the most disgraceful decisions that ever came down, in the sense that it gave a monopoly to existing copyright holders for nothing. And when you are running a bargain, you don't want to have those retrofittings going on here. So again, I want to know something about the mechanisms, not about the aspirations. At this point, God lies in the details and the plumbing, and until I see the way the pipes are put together, I can't tell what's going on. I'm putting myself in the position of

the consumer, and from what I have learned about what this conception of what the Broadcast Flag is, and does, and how it operates, I haven't heard enough to be able make a judgment. Until I have more information, I think everyone will be extremely skittish and skeptical of what should be done.

BERMAN: Well, let's explore a little bit. A lot of the comments on the Broadcast Flag were for it, and then a lot said it's ineffective. I don't think that is responsive. Who controls and makes decisions about the technologies that would create a market of technologies that would recognize and permit over time a range of other uses and permissions that are not a copying of millions of copies over the Internet? For example, the technology and encoding rules that would allow the Internet to be part of the home entertainment network—right now, as I read it, Fritz, the rule would say that three studios would have to agree that the technology is robust and compliant. Isn't that a little close to giving the power over the technologies to the incumbents?

ATTAWAY: Jerry [Berman], unfortunately you engage in selective reading. You are right, that is one of the criteria, but it is one of four. There are other criteria, as well. One of which is technology that is equally effective as what is already on Table A, and I would say that is a very objective criteria, one that the FCC can easily measure. It is open to absolutely any new innovative technology, so long as it is equally effective; and I would also like to point out some of the irresponsible rhetoric you have no doubt heard. The Broadcast Flag only does one thing: it only prevents the redistribution of digital content over broad digital networks. It has no effect on copying whatsoever. You can make all the copies you want to. You can do anything you want to with those copies. You can make copies of copies. It does not affect copying.

HEALEY: Could I jump in on that? One of the impacts though, correct me if I'm wrong, is that in today's digital networking technologies, there is no way to have Ethernet in play. Basically, the digital connection would have to be encrypted, so if I have Ethernet set up in my home, and I want to move video—broadcast digital video—around that network, which I imagine people are going to want to do someday, I couldn't do it with Ethernet. I'd have to come up with a different technology.

ATTAWAY: Using today's technology, yes, you are correct, but I think that will change very quickly. I think there will be secure methods of moving content on Ethernets, and even over the Internet by e-mail. It's just a matter of developing the technology to do that, and we have no problem with that. Our only problem is the mass redistribution of content to tens of millions of people over the Internet, which destroys the aftermarket for television programs.

BERMAN: Fritz [Attaway], with copying, let me ask you this. We've been having a dialog with CET, and Consumer's Union, with a range of companies and across sectors, but we get different answers to different questions , and I'm not foreclosing that the Broadcast Flag is wrong, but take this example, and I get different answers: Pam Samuelson appears on Nightline to talk about copyright within the flag structure. I want to take a snippet, and put it on a compliant computer, and I want send it to someone downstream. Not the whole Nightline, and maybe it shouldn't even be flagged, but I want to send that snippet to her office. Can I do it under the Flag proposal?

ATTAWAY: Yes, if the technology exists for you to do that securely.

THOMPSON: Maybe this highlights a bit of the problem, because the question is, "When does a grant of any sort of intellectual property rights happen?", which I do think is a monopoly, and a legal monopoly. When it bleeds over into non-infringing uses, that's when you have an innovation problem and a competition problem that gives me great pause, because then consumers don't even know what they are not getting, they don't know what they are not seeing, they don't know whether they could have gotten something cheaper either. So the question is whether you use a blunt instrument to get to a pinprick problem. Now I'm not going to say that there is a de minimus problem here, but what I am saying is, it gives me a bit of hesitation. This is an area where I have not formed judgments, but the answer is not 0 and the answer is not 100. It's somewhere in between, and it has to have some flexibility. And I'm worried about when you wind up creating standards that at the outset wind up appearing to be overbroad.

ATTAWAY: I agree with you. The tools are often more blunt than you would like them to be; but let me give you an illustration of a balancing test. The DVD. It is true that certain possible uses of the fair uses are not possible because of the Content Scramble System. However, the Content Scramble System was essential to induce movie owners to release their product in that environment. The DVD has become the most popular consumer electronics device in history. Millions of consumers are enjoying movies, in a way that they never had an opportunity to do so before. So you weigh what consumer benefit was produced by the DVD, against what consumer negative impact there was, which I submit to you is de minimus, and consumers are a whole lot better off today than ten years ago when the only home video source was VHS.

THOMPSON: Let me point out some issues. It strikes me, that the potential chilling effect, as mentioned by Congresswoman [Lofgren], if you wind up selling product that could potentially harm machines people have,

and you fail to disclose it, that's problematic. So I can't think of that as being a good thing. But I'm going to take a step back even further. Two years ago, when I was looking at the merger of AOL/Time Warner, and we were looking at Time Warner owning monopoly cable power over 22 large markets in the U.S., the movie industry and others asked for us to put some strong conditions, so that the people providing the pipe weren't able to have a chilling effect over innovation by jiggering with standards for sets with set top boxes, so that there could be a variety of ways that content producers could get into your house. Now, how am I supposed to respond, when those very same producers come back and say, "Yes, so long as it's done our way"?

EPSTEIN: Ignorance is bliss, I think, on many of these panels. As best I can tell, the objection against the Broadcast Flag seems to be at this particular point that it will stop fragmented use that would normally be protected under the fair use doctrine. I haven't heard any kind of other monopoly arguments, and if that's where it sits, then I guess I'm with Fritz [Attaway], although, two seconds ago, I was against him. The problem with fragmentation is, I think, much more serious. You get ten people who want fragments, and they each take ten minute fragments, and then somebody could reassemble the movie on the outside, and the difficulty that you have to remember is that he is working in a precise environment, and if he loses one pristine copy of a DVD to an unauthorized network, then he's lost a billion copies to it, and so when you start saying there is just a small breach in the wall, this is an industry in which everything cascades instantly. It seems to me that if a Flag can do what he says, and does nothing more, and I don't believe this yet, because I don't know enough about the technical stuff, but if that's the representation, you don't have the problems that you have with the Hollings situation, where you are mucking up computer hardware, which compromises the use of all sorts of nonprotected software. What is needed is a remedy that is software specific and content specific, rather than machine general. Therefore in effect, that should be the path we go down, and we should be pleased that at least in the first instance, we've got Hollings off the table. Now you can tinker with this thing, but it's a question of doing it all in his way, or doing it none, because if the fair use leakage becomes essentially a complete stream, then I would rather give up that little bit of consumer right in order to keep the instruments working.

BLACK: Let me try one more on this. The problem is not the technology of the Flag being inserted, or companies trying to say, "Here's what we think should be done." It is that there is a specific solution, investing huge power in a small group of companies. We see ways in which it can

have an impact steering technology, choking off viable alternative options for technology, in spite of Fritz [Attaway]'s saying "Well, there can be similar functionality." Yeah, we can end up in litigation for lots of years. In the interim, you will be in a situation where lots of people will be chilled from going in those alternative directions.

SAMUELSON: As I understand it, part of the concern is that the Broadcast Flag doesn't just constitute a regulation of TV tuners. It will also affect modulators and demodulators, and downstream devices, and to the extent that motion picture companies have the power to say "yea" or "nay" to the development of these technologies, that, I think, is the concern.

ATTAWAY: There is no proposal on the table that gives us that power. I don't know what the source of that statement is.

SAMUELSON: Well, Emery [Simon] is actually in disagreement with you.

SIMON: That's not very accurate, Fritz [Attaway], because the motion picture industry has identified universal problems of piracy, of which the Broadcast Flag addresses one, and that's free over-the-air digital transmissions. But there are lots of other sources of leakages, and the model that is, or is not, put into regulation, undoubtedly will create precedence for how subsequent piracy problems will be resolved. Moreover, we know that five years ago, p-to-p piracy was not something we were aware of, and today it's a huge issue, not only for the movie industry, but for the software industry as well. I can assert with full confidence that in five years it will be in yet another form. The piracy problem that studios confront, software companies confront, the film companies confront, all copyright holders confront, will be a constantly evolving and changing one. The fear of the Broadcast Flag approach is that it sets into motion a regulatory interventionist model, which will then become a model that will have a certain gravitas, a certain center of gravity, proceeding thereafter with these issues. And if you think technology drives your products, and you think technology is good for your industry—and we appear to—by solving the problems with certain bad ways, we end up chilling technology and by that you'll be hurting yourselves in that as well.

ATTAWAY: So your position is that we should not solve a problem that you readily admit exists, because the solution, although itself is benign, could possibly maybe someday in the future perhaps be a precedent for something you don't like? What kind of a position is that?

EPSTEIN: That's not my position.

SIMON: That's not mine either. (laughing)

EPSTEIN: I'll tell you, it's not mine, and maybe that means something a little different to Fritz [Attaway], but what I've heard is a delegation to a private body to set standards which would act as an exclusive barrier to entry to new technologies. That's what I hear. The question one has to ask is: As you hear it, is it true? And I would like someone to tell me whether or not there is a scenario in which, if we give this man and his friends a part control over the lever, he can stop a new form of technology from emerging. I want to know that. I also want to know why it would be in his interest to do such a thing. I don't quite hear the answers. I hear the fears. I don't hear that they are as ominous as Fritz [Attaway] makes them out to be. On the other hand they are not as specific as I would want them to be before I would be prepared to say this technology has too many interests to go forward.

SIMON: Your example is, the premiere example is, the technology that was developed to protect DVDs before CSS came along, which was a technology worked out by the motion picture industry and the consumer electronics industry, and which they legislated. There was a big long bill and a big long standards document that went along with it, and it was a mandate. When the computer and software industry looked at that technology, we came to the conclusion that it would make so many calls on CPUs, so constantly, that performance would be degraded dramatically. So there is an example of a way that you can come up with bad solutions. The way that CSS came about, and the DVD solution came about, was to abandon that approach where a whole bunch of engineers sit down and do the standards process, which is what they do all the time, figure out standards; and when they figured out a standard that worked, people kind of made it into what eventually became CSS. So yes, you can have bad solutions that have substantial negative impacts.

SAMUELSON: Jon [Healey], I wonder if you would say a few words about how you try to, as a reporter, cover stories about things like Broadcast Flags, which involve so many complex technologies and people who have so many different views about what the proposals are about.

HEALEY: Well, I try to understand it as a user would understand it, which means getting past the engineering details as fast as I can, with as little insight as I can bring to bear, because a lot of these things are process debates. My average reader doesn't care about the process, they care about the results. That's not to say the process isn't important. So, the first thing to do is figure out what the problem is that people want to solve, which in the Broadcast Flag instance, was all about Internet redistribution. This is a problem for us, but wasn't much of a problem until Napster pointed it out for the music industry, and sort of by assumption or extrapolation, the

video industry figured it would come to them as well. So after that, you have to look at what technologies might be out there to solve the problem. In this case of the Broadcast Flag, the standard setting body for the TV industry, the ATSC (Advanced Television Systems Committee), had already identified a set of bits that could be used to act as a trigger, right? So then it became a policy question. That's the hardest part of my job: seeing all the ramifications of the different policies, which also means understanding in a better way what the problem is. Because everyone is concerned, I think, in the Broadcast Flag debate, not about solving the problem. There is an agreement that unauthorized Internet redistribution is an issue for the video guys that needs to be addressed. What they are concerned about is that if you take steps A, B, and C, then what happens? It's almost a test of your imagination, because we don't know what's going to happen.

BERMAN: One last comment. I really think that we have to explore how this Flag or any of these standards are going to work and we have to get inside the game and inside the process, and unless people can ask questions, and not have their positions construed one way or the other.

SAMUELSON: So an alternative to the FCC or Congress doing mandates through legislation or regulation, is the private standards setting process, and I want to come back to a question Jerry [Berman] posed a little bit ago about the public interest and standard setting organizations in context, because very often the people who engage in these standard setting organizations tend to be big players with stakes. The question is: Is there a way for those processes to be open to public interest representation?

SIMON: Well, first of all, I have been involved in these standard setting bodies. The answer is that they are open, so any public interest group can show up, but what you are identifying is actually a tension in a hard question, which is how a public interest group may engage in an exercise that is expensive and time consuming and requires specific engineering skills and know-how. It's a hard thing to do. So if you are going have to a voluntary industry and private sector led standards setting body, for public interest groups to participate in, that is a tough thing. The alternative is to do it in a public interest forum, like Congress or the FCC, which then generates the alternative problem of legislation or regulation. So there is a tension between those things. For my money, it's still better to try to do this through voluntary efforts, and include whoever wants to show up at these meetings and speak their minds.

BERMAN: I really believe that my organization has fought against government mandates from the DEA and from export controls, and we

want to avoid as much regulation of the Internet as possible, yet the irony is that the only place where we have a voice right now is at the FCC, which is trying to regulate Broadcast Flags. Emery [Simon] raises a very serious question: if we want to participate in it, it's open, but it takes money, resources, and so forth. That barrier has to be crossed, because otherwise there is no chair at the table. But what is the other side? Let's say we can cross that Rubicon. There is a second point for consumer organizations: if you get into the process, you got to be in good faith, attempting to work on the standards, and trying to make it work; and there are a lot of people in this audience, who believe that if you get into the details, whether snippets for fair use, or anything else I can think of that you are on a slippery slope, and you are therefore going to end up endorsing the process. So if it's a zero sum game, consumers will not, they can't participate. If they are going to participate, they are going to have to get into the weeds.

ATTAWAY: Jerry [Berman], there is another safeguard that you are not addressing. Emery [Simon] is right, these standard bodies are open, but Jerry [Berman], I agree with you, sometimes it is inconvenient or even impossible for consumer groups to participate. But there is a very effective safeguard for consumers in place. It's called the marketplace. If standards are set that are unacceptable to consumers, they will be rejected; and they are, frequently. You see it every day. Technology is put out into the marketplace, consumers don't like it and it dies.

EPSTEIN: We are not worried about that. We are worried about the stuff that doesn't get out into the marketplace. The problem is I don't know who fills this chair where the public is supposed to sit? It seems to me you have large numbers of individuals, and there is an aggregation problem, and the traditional methodological individualist, as I am, says the only way you get to social utility is to sum individual utilities, such that the public is only coalitions and groups and so forth. And so hearing that there is some sort of mythical override leads me to fear again that there will be some sort of saving dictator who will be able to protect us all from ourselves, which will lead to our own ruination. The time to figure out how to work this process is going to be very, very difficult, given that constraint. I want to know whether you are strengthening markets or strengthening monopolies. There is a long history in the law, in every area from imports on down, where safety regulations are used, in my view improperly, to protect yourself from monopoly. I don't know whether that is happening here, and until someone answers that question, I don't know where to cast my ballot.

SIMON: Let me confuse things with the facts. So you say, where is the evidence that the marketplace will respond? The software industry has used DRMs for twenty-five years. It goes through a cycle. The software industry tightens up the DRMs and consumers scream, because they can't do very much with the software when it fails, or they want to reload it. Companies loosen up on the DRM, and the piracy goes way up, and then they tighten up on it. That has been the cycle, and that continues to be the cycle, and we're reconciled to that cycle. What we do in that cycle is we abandon technologies that consumers hated the worst. I'll give you an example. There is something called a dongle, a little piece of hardware that people attach to the back of the PC with which the PC has to shake hands in order to run the software. People hated it. Nobody uses a dongle anymore. So yes, there are DRMs that are hated by the marketplace, and are taken out of the marketplace in response to the market.

BLACK: To answer the question about standard-setting processes. First of all, there are thousands of standards created all the time. If the standard setting body tends to be dominated by a few very large players, the temptation to use the standard not to create an open standard, but to create a competitive disadvantage for potential competitors, looms large. I think with the Broadcast Flag we see this, I see that as part of the problem. But in general, I would love to see consumer interests able to be more vigorously represented more often. To the extent if we have a highly competitive group of players in the standards setting process, there is a certain amount of capability of the marketplace for the consumer voice to be somewhat heard, but when you have a smaller subset, when you have big players, that's when you have the potential for this.

HEALEY: Who should decide which programs can carry a flag? One might argue that the best place for those policy decisions isn't, to borrow the phrase from the Microsoft presentation a couple of days ago, "Isn't with the technologists, it's with the policymakers."

. . . .

THOMPSON: This is where I'm here to help you. (laughter) It is important to have, and this is something I've talked about that's involved technology issues, which may make this particular area a little different than some of the others that the government works in, that no one group has the answer. So it's important to have a diversity of views, and it's important to recognize that those views may not be fixed in stone, and they can change over time. Now, the marketplace is a great force but sometimes that market is not perfect. Otherwise, you wouldn't have people like us who are involved in antitrust issues, or consumer protection issues; and we are not regulators, we are law enforcers, which means that the market

works most of the time, but every once in a while you have to kick it in the butt, because there are some course corrections that are necessary. That gets us to standard setting. We have a presumption that standard setting organizations are good, to the extent that they can bring rationality to a given marketplace, and provide some efficiencies, so consumers benefit. The question is: Are there circumstances under which standards setting organizations become corrupted, by not full participation ?

I would also say that I would not be so quick to characterize public forums that are sponsored by government as simply those that wind up legislating or rule making. We at the FTC are having a workshop on spam in a few weeks. We had one on privacy technology. We had one on B2B marketplaces, where we take no action, and we took the step of saying we were taking no action, because we wanted to see it develop. So I think that we can actually form a place where we can talk very candidly, and perhaps get a little less positional, and perhaps more in the problem-solving mode.

BERMAN: That would be very, very helpful. In other Internet areas , the ball has been driven forward by the government providing a forum for getting people together. I think that would be a terrific role for the FTC, not a regulatory role, but just a convening role, a place to go. I understand, the consumer is a check, but there are certain things where the consumer is not dispositive, and the most important is in areas of free speech and privacy. Those are rights, which may conflict with majority opinion. The majority may love getting Harry Potter, but they may not care if all news and public affairs are flagged, and not available. I think that those issues have to be addressed, because if we are going to be in a closed system, and rely on future technologies, should some content be unflagged? On First Amendment rights alone, I think there is a serious issue about whether public affairs should be flagged.

ATTAWAY: Jerry [Berman], you once again mention the First Amendment and free speech, despite the fact that court after court after court has said that free speech does not mean you have the right to take someone else's speech and use it. The First Amendment has nothing to do with what we are talking about here.

SAMUELSON: I've read those cases and that actually isn't what they said. (laughter)

THOMPSON: This gets to the instance of the overbreadth that I've been talking about, in the sense that I've heard the same thing when we are talking about what constitutes commercial speech as well. So when the business community tells me that they can use information for whatever purpose, that's not true either. So it's important to try to get to the middle of what's reasonable. I always like people who cite the First Amendment

on the one hand and then on the other hand, at the same time say that's reserved for lawyers.

SAMUELSON: So I think it's time to go to a controversial subject, perhaps some discussion about the anticircumvention regulations, since Congresswoman Lofgren was here talking to us in part about that. As was mentioned yesterday, a preliminary injunction has been issued in the *Lexmark* case against Static Control's continued ability to sell their toner cartridges. That case, and the *Chamberlain* case and the universal garage door opener, are DMCA claims that I think are unintended consequences. The question of whether there might need to be some tweaking of the anticircumvention rules to exclude these kinds of cases from the scope seems like it might be worth talking about.

BERMAN: I think that there are several areas where the Congresswoman agrees that there needs to be tweaking, and we could maybe agree on some of the tweakings, but here is where I have to make two points. Unless consumers are really organized with the technology community, and get into the game, Representatives Lofgren and Boucher are flying alone, and they are not going to be able to tweak the DMCA. There are serious interests who don't want to open up the DMCA for very good reasons. It protects their software, it protects their content, and they are not interested in opening that to the political realm. Even if they agree that changes need to be made, they are not willing to take the risk. That has to be created by others, who want to make those changes, organizing, coming in and trying, and delivering political power, not market power, to put those issues on the table. I don't think we are anywhere near it; and when Larry Lessig says in the face of the Flag, the DTV bill, the need to wrestle with fair use, a standards body, and draw an X through Congress, and says, "Let's go somewhere else now because we lost the *Eldred* case"—I think that is a fundamentally wrong message. If you want to affect these policies, you have to organize, and you have to be in Congress, and they have got to hear your voices, because the reality is, the content people are well known, they have a lot of power, and they have a very good case. They are very worried, in particular the movie industry. They don't want what happened to the record industry to happen to them. They have an enormous amount of power, and I think they have a very good case, but the balancing of that case requires a lot of work by consumers, and the consumers, including us, are not sufficiently there.

EPSTEIN: I am a little bit mystified. What happens is you build up a huge head of steam, and you may take care of the garage door opener case, which does or does not matter, or these compatible systems, but any legislation you are going to enact will have massive movements in the opposite

direction. If this is the extent to which we have a problem, my own strong inclination is that I will listen to any side in the face of judicial format to see whether or not there is an implied exception, to see if the cases get reversed, but I don't think two swallows make a summer. There are billions upon billions of interests on the other side, and the moment you start to create a crack in the other side, you make a crack in the edifice of protection, and the whole wall comes crumbing down. The discontinuous nature of this business is something that leads one to think that they are attractive in principle, in an abstract way, but terribly dangerous when you are trying to implement them, because there is no way you could break the flow. The slope is simply too steep.

ATTAWAY: I don't want to sully Jerry [Berman]'s reputation, but I'm going to agree with him. Do you mind? (laughter). The bill that was introduced by Congressman Boucher is not tweaking the DMCA. It repeals the DMCA. The essence of the DMCA, at least for us in the motion picture industry, is the prohibition against trafficking in circumvention devices. We realize we cannot station a policeman in the home of every consumer to see if they are circumventing any particular technological measure. What we have to do is prevent the mainstream commercial availability of circumvention devices and that's what the DMCA gives us. Congressman Boucher has introduced a bill that says any device that is capable of allowing fair use is not a circumvention device. It totally repeals the essence of the DMCA. Burglar tools have legitimate uses. You can legally break into your own home, but if burglar tools were allowed in mainstream commerce, the predominant use of those tools would be to burglarize people's homes. The same thing applies with circumvention devices. So Congressman Boucher presented this view in 1998, and it was soundly rejected. He's presenting it again today, and I predict it will be equally soundly rejected.

BLACK: Let me talk a little bit about the history of the DMCA. First, we went back to WIPO, and White Papers before then, and there were many years of discussions by a lot of players, on how to structure this world. There were a number of people in opposition to certain proposals that wound up becoming the law, and believe me, I think the law was modified to a much more balanced position than it started out in some of the early drafts. But circumvention was used, because a decision was made in the process. Either you say fundamentally that everything is to be banned, and you make exceptions for some uses, or you do the reverse, and you say we won't ban stuff per se, but we will itemize and list all those improper burglar tools that can be identified, and create a rapid way to identify them. So it was really which side of the presumption and where

the exceptions were. Many of us argued that in a rapid and changing technological era, that it was really wrong to say that there was a blanket prohibition on devices, when we knew what was going to be out there, that anticircumvention tools that might inadvertently be structured in such a way, that totally innocent products could have an effect of looking like a circumvention tool. So facing that unknown world, none of us wanted that to be. We were going to be very liberal in identifying something that was going to be misused, we'll deal with it, we'll list it, but in fact, we had the opposite effect, and we basically are living this now. Even now with the exceptions, which are modest, were fought tooth and nail for. Research, and no one even thought of encryption research as an exception two months before the bill was passed, surfaced and it was fought for tooth and nail. I am in agreement with Emery [Simon]. There was no broad understanding in Congress with what they were doing. These were nitty gritty little debates that were fought out in the trenches, and the impact, we think, is as we predicted: Far-reaching consequences of people coming to use the anticircumvention provisions for anti-competitive uses, not for intellectual property protections purposes, and that's the danger.

. . . .

THOMPSON: I think that what was raised earlier about what kind of public voice there is, I won't diminish the value of that public voice. I mean sure, there is a lot of money, there are a lot of interests out there, but that's not to say that the interests of consumers or end users are not important, or to the extent that they are organized, that they may not be able to get at the legislative bits. But they sure can inform the legislature about what is going on, and they surely have a role in informing people like us, when people who legislate ask us what our opinions are. So knowing what happens out there on the ground, including what the side effects are, is important. For example, a lot of people don't know, and they should know, that one of the principle tools in antitrust are squealers, people who are competitors and who see things that are going on that we might not be able to see. Then we get a chance to sit down and think about what the impact is. I don't want to preach those issues, but that's why I would have some reservations about talking about what the scope of legislation might be, or what a fix might be because none of us have a total picture.

SIMON: Let me try to answer your question, which is about *Lexmark*. Whether it was an unintended situation under the DMCA or an unanticipated one, I don't know. What the DMCA is focused on is the piracy issues, and so it was not based on relationships between companies, competitors and the marketplace. So it was certainly an unanticipated situation. Whether the DMCA should be used in that way or not, I personally think

it should not, but whether it will or not, the courts will decide; and ultimately, if the courts decide this thing erroneously, there will be a role for coming back and looking at this thing again. On the things that Zoe Lofgren talked about this morning, I think one of the most revealing things was a question that was asked yesterday afternoon to a group of technologists: "Do you know, as a matter of technology, how to create a set of technologies that will permit fair uses without letting everything out of the bag?" The answer from three of that panel was no. I'm not diminishing the importance of fair use or private use or individual interests or anything, but if you don't know how to fix that problem with technology, if you fix it as a matter of law, what you have done is you have eviscerated the very purpose of the statute; and that seems to me a little bit of overkill.

EPSTEIN: This is a completely discontinuous problem. To think that what you would want to do in order to preserve fair use is to decimate an entire industry, or two industries as the case may be, strikes me as being an extremely odd kind of conclusion to reach. I don't see where the intermediate fix is, because once one pristine copy gets out, then there are a billion pristine copies that are out there, and one has to realize that there is this precipice, which I think determines the shape of the entire debate.

BLACK: The premise is industries are going to be destroyed. We've heard that over and over and over and over.

. . . .

EPSTEIN: It's not that the technology constrains the set of intermediate choices we have today. This is not fair use in the traditional sense of literary criticism that you need to make with somebody else's work. This is fair use in the sense of reproduction for private uses, and unless someone can explain how you can make one copy without making ten billion copies, then the issue becomes a very serious one. Is it Armageddon?

BERMAN: Richard [Epstein], there are ways to do that. You have not asked for explanations. You have just said it's not possible, therefore let's not explore it. But what Mozelle [Thompson] said is that whether it's the DMCA, or what can be done about fair use, the only way to get out of extreme characterizations—either legislative proposals—is to sit down and talk about the facts and how the technology works. You've made some assumptions about the technologies that are not true. You need to know that it would take 17 hours to put Harry Potter together. So those facts need to be discussed. The forum is missing. It is totally adversarial. One of the problems with Congress is that while they are holding hearings, the level of knowledge about the Internet—you can count on your hands the number of Congressmen who know that it is not similar to a television set—that is a serious problem because they will legislate. So creating

those forums, creating ways to bring the industry, the technologists and the consumers together, is absolutely critical to get out of this kind of problem we are having.

SIMON: Let's look at the fair use concept, and the fair use concept is a public interest, public policy balancing statute, which essentially says that if you are going to do something socially redeeming, like research or like education or like something socially redeeming, we'll excuse the fact that you've made unauthorized copies, and that's a good thing. So now we look at the overall context that the anti-circumvention rules appear in, and you do a balancing test again. On the one hand, you balance the potential threat, it's not an absolute threat, and probably Richard [Epstein] overstated it, but it is a serious potential threat. You balance against that the public interest that is inherent in the balancing of fair use, and you come up with an answer. The problem is that it is not going to be the same answer in every situation. I believe that the DMCA, for the moment, has gotten it about right, and I believe that doing what Zoe [Lofgren] and Rick [Boucher] and others propose would be a mistake. It's too early to make those decisions. Let's let it play out a little bit longer. Let's have some proof of the fact that there is really a lot of harm going on here, because frankly I haven't seen all that much.

BERMAN: I agree, I'm all for the documentation. Let's document and talk about the facts within a forum. And fair use is a balancing task, but within the constraints of DRM technology, where the possibility of exercising it, and then defending it in traditional fair use terms, may not be possible, so that you are on the end of asking permission for taking a snippet , that is a fundamental change in the way fair use works. If that's true, then you have to find a way, a forum, of how to rebalance those things, because there is no way to do the balance, if you turn it on its head and make it a permission.

HEALEY: Aren't we presupposing that the universe gets DRM? I mean, if there are non-DRM sources of content in the marketplace, and the public doesn't like the DRM sources, then you would think the non-DRM sources would win, and that would provide your outlet for fair uses and other uses that DRM content would not provide.

SAMUELSON: I think that is one of the things Larry Lessig was trying to envision with his Creative Commons initiative. I actually want to open it up to questions from the floor. Don?

QUESTIONER, DON WHITESIDE, INTEL: You might think of CSS as an imperfect solution that had great benefit for content providers and consumers six years ago. We are now at a point where we can actually expand CSS to enable portability. I am curious when we will see an update

to the CSS license to allow protected outputs to DRMs that exist and other protected environments very similar to what the cable industry just announced ?

ATTAWAY: Don [Whiteside], I wish could answer the question but those are decisions that are way above my pay grade. I agree with you that they need to be made. I am not involved in the negotiations aimed at reaching the resolution, but I hope that a resolution comes quickly.

. . . .

QUESTIONER, MARK LEMLEY, BOALT HALL: So, the consensus, to the extent that there is any consensus on this panel, seems to be, the Hollings bill is a bad idea. Why is it a bad idea? Because it mandates the way we build technology, and the market is generally the preferable solution. My question is this: Why then is the Broadcast Flag at the FCC? I would expect a market-based solution to be one in which device manufacturers, perhaps at a standards setting organization, but not uniformly, compete to make devices that do, or do not, encode something, right? And if they are in fact concerned by what Fritz said at the beginning, which is that we will not send content for free, unless these devices exist, I would expect the market to develop such a process on its own. The fact that we are not at the market, that we are instead asking the FCC, I take it, to mandate something along these lines, suggests to me that what's going on is not any kind of market driven, or even standards setting process in the classical sense, but instead regulation. Maybe there is a good reason for that, but if there is a good reason for that, then maybe we have to decide what that is. But we have to abandon this pretense that we are in fact doing anything different, and we have to come out and say that we are regulating technology, and this is why it's a good thing.

SIMON: Well, it is in fact a good thing; and the reason is that the marketplace way to solve this problem is for broadcasters to encrypt their signals and operate the same way that cable and satellite delivery systems do, where the broadcaster can control the types of devices that process their signals, and require those devices not to pass that content onto the Internet. However, the policy implications of doing that are rather extreme. It would immediately render useless every consumer digital television device that has been sold in the marketplace.

. . . .

LEMLEY: We don't want to do that because it would prevent a bunch of devices from being useful, but perhaps what is happening is that the market is solving the problem in a different way, right?

. . . .

I think you can make an argument for regulation, but I think you have to make an argument for it as regulation. You've got to abandon this pretense that Broadcast Flag is a market-based solution to anything. You've got to say, "we need regulation to solve this problem, government please help us."

SIMON: I'm sorry if I gave the impression that we don't think it's regulation. It is regulation, absolutely, of course it is.

EPSTEIN: But Mark [Lemley], I think the difference between this and Hollings is that in one case you are trying to control the show, and in another case you are trying to run the box. Therefore, the level of interference under Hollings is at least presumptively higher than it is under Broadcast Flag, and what one has to do is to go into the details to see whether or not that statement is true or false.

. . . .

QUESTIONER, LUCKY GREEN, CYPHERPUNKS.TO: I do have a question about the Broadcast Flag, and its potential anticompetitive consequences, not in the content space, but in the HDTV receiver space, and this question is really going to the FTC. There are currently HDTV receivers that are quite expensive. It's one of the many reasons why high quality television broadcast is not being received by many in the American television population. There are currently projects underway at present, software-defined related projects, that permit the receiver to get HD reception, and it is a fraction of the cost of any computer-based solution currently on which the market is based. Needless to say, this is all done with software, and since the software is all being given away in source code form, downloaded from the Internet, the robustness requirements that necessarily would accompany the Broadcast Flag cannot possibly be met. Hence a considerably less expensive technology would be of obvious consumer benefit, would be kept off the market, if a Broadcast Flag were to be implemented. So I'm wondering: Is this truly in the best interests of the MPAA, for HDTV receivers to be four or five times more expensive than they could be, and what does the FTC have to say about that?

ATTAWAY: HDTV receivers are going to have to be able to process protected content. That's totally separate and apart from the Broadcast Flag issue. People are not going to invest in an HD receiver only to watch over-the-air broadcasting. They are going to want to watch cable, they are going to want to watch satellite, going to want to watch DVDs, they are going to want to watch premium content that is protected. All the Broadcast Flag would do is to say that off-air content has to be routed through a protected interface that is going to be there anyway because it needs to be there to render all of this other content that will be protected; and consum-

ers will not be able to watch, unless they have a device that can handle this kind of content. So there is no additional cost. The protection has to be there anyway to receive the other kinds of content.

HEALEY: What about the professor's remark? Can you make, using software, an HDTV receiver that meets the robustness requirements of the Broadcast Flag?

ATTAWAY: I'm afraid I went to law school, not engineering school.

SIMON: Let me try to answer that, because I was involved in that process. So the answer is: we haven't agreed on what robustness rules should be. There is a proposal in front of the FCC, but that doesn't mean there is consensus on what the robustness rules will be. If we were to agree on what those robustness rules are, then our experience in the past has been that yes, we can deploy that software. I just want to come back to one important point raised. The right way to protect Broadcast is to encrypt it. The reason why the music industry has a huge piracy problem is because their product is out there in the clear. The reason why DVDs will go with CSS: it's not in the clear. When you put out free over-the-air broadcast in the clear, you are asking for trouble.

. . . .

SIMON: Do you know what percent of the American public who gets their television that way? Less than 20%.

EPSTEIN: Well, then you are telling me something which I kind of guessed, because I have cable and a dish at my house. I get anything I can get over-the-air, with those two things. So what we really have to do is to junk that technology, put everything through encryption. Once you encrypt it then you can monitor it, once you can monitor it; then you don't care about the assignment problem, and then we can all go home, including the FTC.

THOMPSON: With all due respect, a lot of people like me are among those 20%.

EPSTEIN: It's like Life Magazine, where it turns out that there was a time when picture magazines were great, but then television came along and they could never quite recover their market share. And what will happen is, if in fact we adopt the technology, you as a private citizen will adapt more rapidly than you as an FTC regulator.

SAMUELSON: I think this is an extraordinary moment to close. Thank you very much.

V. ANTICIRCUMVENTION REGULATIONS IN THE UNITED STATES AND ELSEWHERE

Panel:

Mark Lemley, Boalt Hall School of Law, University of California, Berkeley (moderator)

Tony Reese, University of Texas Law School

Graeme Dinwoodie, Chicago Kent Law School

Bernt Hugenholtz, University of Amsterdam, Information Law Institute

LEMLEY: Our final panel of the day continues what appears to be today's theme, of anticircumvention regulations and their relationship to Digital Rights Management. However, we are doing something shocking and novel for a conference based in the United States, which is that we will broaden the focus beyond the United States and actually talk about regulations and potential regulations in other countries. To lead us off, Professor Tony Reese of the University of Texas School of Law—and special counsel to the law firm of Morrison & Foerster—will talk about anticircumvention regulations in the United States, and their relationship to Digital Rights Management. He will be followed by Professor Graeme Dinwoodie of Chicago-Kent School of Law, and Professor Bernt Hugenholtz of the Institute for Information Law at the University of Amsterdam, both of whom will talk about anticircumvention regulations in European countries.

REESE: Thank you, Mark. My time is brief, but I would be remiss if I didn't take part of it to thank Pam Samuelson for inviting me, and to thank Pam and her colleagues and her students and the other co-sponsors for putting on this truly terrific and illuminating event.

I am going to be talking about a paper that I wrote that is available on the conference website. The paper raises the question of what incentives the legal protections for DRM systems that are in copyright law today offer copyright owners who are choosing which DRM systems to deploy. Now, I realize that legal considerations may be a fairly minor consideration in the choice by copyright owners of which technological protection measure to use. They are also going to be looking at how efficient and effective and costly those systems are. But I'm a lawyer, so I look at the legal regime, and I think that given the fact that copyright owners fought very aggressively for the anticircumvention provisions, and as we saw earlier this morning, speak very strongly about them, it is reasonable to think

that they will play some role in the choice of which DRM systems get deployed.

So, to remind you briefly of what Pam told us all at the tutorial on Thursday, the law in the United States protects two different kinds of technical control measures: access controls, measures that control access to a work; and what I call rights controls, measures that protect the rights of the copyright owner—the right to reproduce, distribute, publicly perform, publicly display, and so on. These two different kinds of controls get different legal treatment under the statute, and access controls seem to get more protection than rights controls. The clearest way that that is true is that access controls are protected against acts of circumvention, and rights controls are not.

Let me give you an example. The paradigm example of an access control might be something like the Divx system, where you buy a disk and the system allows you to access it only on a certain machine, and only for 24 hours, unless you contact the copyright owner and pay an additional fee. If Divx were still in existence, and you hacked around the protection in order to watch the film after your 24 hours had expired, that would be a paradigm instance of circumventing an access control. That act is illegal under Chapter 12 of the Copyright Act.

Rights controls, on the other hand, are not protected against acts of circumvention, and let me give you an example of how that might work. Imagine that I have a DVD player in my laptop computer, which allows me to play the DVD, see the film on the screen attached to my laptop, but doesn't allow me to send the output signal of the DVD to an LCD projector so that I can show it on a screen. That looks like a rights control. It's not controlling my access to the film, but it's limiting my ability to exercise one of the rights of a copyright owner, the right to publicly perform the film. If I were to circumvent that control (assuming that I had any technological ability, which I don't) in order to send the signal to the LCD projector to show the film on a screen, I would be committing an act of circumvention of a rights control, but not violating the law in any way with respect to the anticircumvention provision, because acts circumventing rights controls are not illegal. If I did that in order to send the signal to a screen in front of my class in Copyright Law at the University of Texas, I would also not be committing any act of copyright infringement, because the Copyright Act expressly allows teachers to publicly perform movies in their classrooms. So, that kind of act of circumvention would not be illegal as a circumventing act and there would not be any liability for it as copyright infringement.

For those reasons, access controls seem to get stronger legal protection in Chapter 12 of the Copyright Act, and that suggests that a copyright owner who wants to maximize the legal protection for a digital rights management system would be well advised to adopt access controls to get this additional protection.

Now, it turns out, if we look at least at the case law under the DMCA anticircumvention rules, copyright owners may not have to choose between these two types of legal protection. They may not need to choose because they may be able to merge access and rights controls into a single system. They may be able to protect against unauthorized exercise of the copyright owner's rights by using an access control.

What's the legal effect of merging access controls and rights controls? Well, so far, the legal effect has been that courts will treat a merged system as both an access control and a rights control, and therefore, entitled to both protections, that is, the stronger protection for access controls against even acts of circumvention. Indeed, in the DeCSS case, the decision of the district court was premised mostly on holding DeCSS illegal as an access control circumvention device. So, by deploying a merged control, the copyright owner gets the benefit of the stronger protection of the access control.

So what? Why do we care if copyright owners undermine this distinction that the statute draws between access controls and rights controls? Knowing whether we care depends on why we treat these things differently. Why do rights controls get less protection and access controls get more? And the legislative history of the DMCA, to the extent it is penetrable at all, is actually replete with statements. "We weren't going to ban the act of circumventing a rights control because that would allow the public to make noninfringing uses of protected works," . . . "If you circumvented a rights control, what you did would be illegal only if it violated copyright law, if it was infringing on its own." So, you could circumvent the rights control, you wouldn't face any liability under the circumvention rules, and if what you did subsequently was not infringing, you wouldn't face any liability under copyright law. So Congress said, "We're treating rights controls differently, giving them less protection in order to give breathing space for noninfringing uses of protected works."

Merging access controls and rights controls, and treating them as entitled to the protections of both, undermines this distinction. Users will have trouble circumventing the rights control, a perfectly legitimate act, without also circumventing the access control, and circumventing the access control is, of course, illegal. So the effect of treating these merged systems as

entitled to both sets of protection is, in effect, to suck all of the oxygen out of this breathing space that Congress tried to allow for noninfringing uses.

So, in the couple minutes I have left, how might we respond to this problem? Well, one response would be to do nothing. We could simply acknowledge that although Congress decided to treat these systems differently, it wasn't really a meaningful distinction. Why might it not be a meaningful distinction? Well, it could be that all the action is really in the device bans, and indeed Fritz Attaway said this morning, what really matters to us in the DMCA is stopping trafficking of devices. We realize that we cannot police these acts of circumvention. So, maybe Congress' intent to leave some breathing space for noninfringing uses by allowing the circumvention of rights controls was just lip service to get the thing passed, but all of the action is really in the device bans.

I am going to credit Congressman Lofgren's suggestion that Congress was in fact not just paying lip service to noninfringing uses. So, the suggestion is that instead of simply ignoring this, what we might do is say that acts of circumvention of an access control measure are not prohibited under the DMCA, as long as the person who circumvents the access control measure doesn't commit copyright infringement. You are free to circumvent them, and any liability that you face would be liability for copyright infringement, not for circumvention. Now, this wouldn't deal with some concerns that people have about the DMCA, which is that the device bans are really what matter, and those of us like me who can't engage in technological savvy circumvention, won't be able to do this even though it's legal, but it's at least a place to start to try and preserve the breathing space that Congress said it wanted to allow for circumvention of noninfringing purposes.

. . . .

DINWOODIE: When the organizers of this conference were putting together the program, a session on the implementation of the EU Copyright Directive seemed likely to be very timely, because the deadline for implementation of the Directive was December 22 of last year. You would think that therefore we would have fifteen or twenty-five national laws that Bernt [Hugenholtz] and I can actually talk about. In fact, two months after that deadline, only Denmark and Greece have actually enacted laws implementing the Directive. While this isn't an unusually tardy schedule, because the European Union Member States don't always implement the Directives on time, it does make what we are talking about a little bit more contingent. The good part of this is that, to the extent you don't like the shape that the proposals currently take, there is still an opportunity to influence the way that Member States implement the Directive in their laws.

The downside is that the Member States are under significant constraints from the European Union legislature itself regarding the choices that they can make about DRM regulation, because the Directive made a lot of those choices at the European Union level, and took away the autonomy from the Member States. That hasn't prevented, at least in the proposals that are out there at the moment, some Member States from trying some creative things, such as defining "technological protection measures" in ways that might exclude certain measures, like region coding and things like that, or adding alternative mechanisms, such as the German proposal does, that would require any product that has a technological protection measure on it to be labeled in a way to allow consumers to know about the content of those measures. The Directive does, however, constrain a lot of the choices, and as Pam [Samuelson] mentioned some of these in the tutorial on Thursday, I don't want to spend a lot of time on them. I should say, however, that like the DMCA, the European Copyright Directive is aimed both at acts and devices. Unlike the DMCA, it does not distinguish in the way that Tony [Reese] talked about between access control and rights control measures. Both are treated exactly the same, in fact, based upon the recognition that in fact these were likely to, at some point, work in combination. One other important difference from the DMCA is that there are no exemptions in the Directive itself to the anticircumvention prohibitions. That is not to say that the legislators were unaware of the potential that a broad prohibition might restrict the ability of the beneficiaries of exemptions under the copyright laws actually to exercise those exemptions; so they enacted a provision, Article 6(4) of the Directive, that really gives voice to that concern, or at least attempts to give voice to that concern.

Let me read the first paragraph. There are several paragraphs in this Article, and Bernt [Hugenholtz] at some step might talk about the second paragraph, but the first one reads as follows: Notwithstanding the prohibitions against acts of circumvention and circumvention devices, in the absence of voluntary measures taken by right holders, including agreements between right holders and other parties concerned, Member States shall take appropriate measures to ensure that right holders make available to the beneficiary of an exception or limitation provided for a national law in accordance with—a whole bunch of Articles that permit exceptions—the means of benefiting from the exception or limitation.

My first reaction to reading that was that it must read better in French. But it doesn't have an awful lot more guidance or clarity in any language of the European Union. What I'm going to try and do is focus on that provision, which really is the vehicle for the infusion of balance into the Di-

rective, and suggest some of the ways in which it might operate, and the ways in which Member States are beginning to consider it operating. Before I do so, let me just mention however, that although it is potentially a very, very broad vehicle, in fact there are some limits built into it at the European Union level. In particular, it's only going to allow beneficiaries of certain listed exemptions to be able to take advantage of the potential 6(4) procedure; and those exemptions must exist in national law. The national laws of the European Union are not really harmonized on exemptions, because the European Union decided to make the list of exemptions in the European Union Copyright Directive optional. So there are significant limits on the ability of Article 4 to provide that balance; but notwithstanding those limits, it continues to operate.

Well, the first question is: What triggers the obligation on Member States to take "appropriate measures"? The provision appears to suggest that the need to take appropriate measures is brought into play by the inability of the beneficiaries of certain of those copyright exemptions to take advantage of the exemptions, because of technological protection measures. Some European commentators suggest that this trigger is unlikely to occur for a while because most works will be available in unprotected formats. If the scope of Article 6(4) was like the DMCA rulemaking, limited to adverse effects on "calluses of works", this argument would seem stronger. But it isn't. If you look at the exceptions that are in Article 5 that are incorporated by reference into 6(4), they refer to uses and purposes, not simply classes of work that are involved.

Perhaps normatively there should be some limit to this. That is to say, perceived unavailability of a single work for a single use might be insufficiently substantial a cost to warrant construction of an entire apparatus or mechanism contemplated by 6(4). Which I guess illustrates the point to some extent that Richard Epstein made this morning. But this depends on what's contemplated by the Member States as an "appropriate measure" in a response to the inability to exercise an exception granted by copyright law. If appropriate measures simply means grant an exemption, then there may not be any real cost to enacting a pretty low trigger level, a low threshold. If appropriate measures means, and this actually is possible and quite clearly contemplated by the Directive, mandating particular technological measures to be used by content providers, or establishing a complex quasi-judicial system for determining when such impairment of ability to exercise such an exception exists, then perhaps a higher degree of impairment should be warranted before that happens. I think the answer actually is that it's a little bit of both. That is to say, Member States should consider the combination of these different devices as ways of assuring

that beneficiaries of copyright exemptions can actually take advantage of those exemptions, and that a combined system using specific exemptions, and a quasi-judicial system not unlike rulemaking, imposing more intrusive or structural measures where classes of works are involved, might actually be the way of doing it.

This, I think, you might say, brings us then to the ultimate question of, what are these appropriate measures that states are obliged to take if, in fact, copyright beneficiaries aren't able to take advantage of exemptions. However, there is still another hurdle here. It's a little more complicated. The obligation of Member States to take these appropriate measures only arises in the absence of voluntary measures taken by rights holders. The recitals emphasized that some reasonable time is to be given to right holders to come up with the voluntary measures. Well, what are the voluntary measures and how do they affect the timing of Member State intervention? The only type of voluntary measure that is expressly referenced is agreements between rights holders and other parties concerned. But reaching such agreements is going to be a very difficult task because of the range of stakeholders with interests implicated by copyright law. To the extent that the exemptions are linked to particular purposes or uses, it is difficult to know who the different persons who potentially should be involved in negotiations are. The likelihood is therefore a complex web of agreements would have to be in place to give full effect to the different copyright exemptions. Rights holders might also consider modification of technological measures in ways that allow the beneficiaries of the exemptions to exercise their exemptions.

I think one of the more interesting things I heard on Thursday, though I think there's a lot of debate within the technological community, is the extent to which technology could in fact be developed in a way that reflects some of the nuances of legal exemptions. My sense was that to reflect the nuances of fair use is close to impossible, but someone made the point that in fact to write down in legal language how fair use applies in particular settings is very, very hard as well; but to the extent that particular exemptions that are actually much more like European exemptions, technology might be one of the appropriate measures that could be mandated by Member States (and which could voluntarily be adopted by rights holders).

The difficulty attendant to the process of voluntary arrangement also implicates the question of timing. Recital 51 imposes an obligation of Member States to promote the voluntary measures we've been talking about, but suggests that rights holders have a reasonable time to develop those measures. Well, what is a reasonable time? Some commentators in

Europe have suggested that such a reasonable period of time should only start to count, only start the clock going, the moment where "technological protection measures are sufficiently widespread and have a negative impact on the beneficiaries of exemptions." On one hand, it may not be clear what future effect the measure is likely to have and acting too quickly may be premature. On the other hand, there is a danger in building exemptions that will apply prospectively based simply on past practices. Those past practices may change. So I think the important thing for Member States to recognize is that there are two different acts involved here that affect timing. One is the obligation to promote voluntary measures, and the second one is Member State intervention by way of appropriate measures to remedy any imbalance.

The first obligation is immediate. As soon as the Directive is effective, that obligation exists. Only the second one is actually delayed. Some Member States in their proposals have understood that and have set up provisions that they think will help promote the development of voluntary measures. In particular, what several states have done is to establish a procedure that doesn't look unlike the DMCA rule-making procedure. In particular, the British proposal suggests that beneficiaries of exemptions who believe that they are not able to take advantage of them can apply to the Secretary of State for a direction to the content provider regarding ways in which the content provider should make the exemption available.

Now that direction may simply be that they have to obtain voluntary agreements with other interested parties. Let me just mention a couple of other possibilities in terms of appropriate measures that are suggested both by the recital and some of the commission officials. Recital 51 mentions the possibility of modification of the implemented technological measures actually being the form of appropriate measures that the state could direct. This interestingly inverts the "no mandate" debate in that content providers might suddenly be very interested in the notion of a "no technological mandate" philosophy. The other thing that I noticed was that one of the top commission officials suggested in a workshop this just last year that these means might include, and I quote, because I'm not quite sure what it means, "handing out the locking key." That's in a translation, so quite what he means I'm not really sure; but certainly the language of "right holders making available to the beneficiary" suggests affirmative conduct on the part of the rightholder, more than simply accepting the availability of the statutory exemption. The extent to which Member States are willing to push affirmative measures as one of the appropriate measures, I think will determine the overall effectiveness of Article 6(4) ensuring the beneficiaries are able to take advantage of their exemptions.

HUGENHOLTZ: I am under specific instruction from the Kingdom of the Netherlands not to make any jokes or other derogatory remarks about your President, so I will be brief. I would like to talk about something distinctly un-American, a typical product of old Europe, which is levies—levies for private copying —and the way the levy system in Europe is being affected, or will be affected, by DRM. Interestingly, while levies appear to be on their way out in Europe, there is increasing interest for levies here in the United States, at least in academic circles.

DRM and levies are from two different worlds. Reconciling them is like trying to square a circle. Indeed, this is what the European Copyright Directive attempts to do. Whereas DRM is based on individual rights management, reinforced by contract and technology, levies are a very crude form of collective rights management. DRM aims at keeping content exclusive, whereas levies operate under a statutory license. Users of DRM-protected content paid for what they get (or not get), whereas levies are something of a tax on equipment media, unrelated to the value of the actual content. Consumers pay providers of DRM based directly, whereas levies are paid by equipment manufacturers, or manufacturers of blank media. These costs then are passed on to the consumers. So, these are very, very different worlds.

Let me tell you a thing or two about private copying levies as we have them in Europe today. They are not the same everywhere. In fact, in the U.K. and Ireland, they do not exist at all. There are levies on equipment in a couple of countries in continental Europe. These levies traditionally apply to photocopying machines, fax machines, tape recording devices, and VCRs. More recently, and more controversially, levies have been imposed in some European countries on digital scanners, MP3 recordables, CD writers, and hard disks. Levies on blank media have also existed for some time: on blank audio and video tape of course, and more recently on minidiscs, CD recordables, CD rewritables, and even on recordable DVDs. So there are lots of levies in Europe today.

It is interesting to have a brief look at the history of the levy system. Levies were invented by the German Supreme Court in the 1950s and ’60s The Court on several occasions held that copying for personal use, using such “modern” technology as tape recorders or photocopiers, was not exempted from copyright protection. Manufacturers of such equipment were therefore held liable for contributory infringement. The Supreme Court, however, also recognized that enforcement of copyright claims against individual users would easily conflict with the users’ right to privacy. Thus a system of levies was suggested as a compromise between copyright and the right to privacy. This court-invented system of levies was

eventually codified, first in Germany, and later in many other countries in the EU.

Now, let's have a look at the EC Copyright Directive, and the way it tries to square this circle. In Articles 6 and 7 it promotes and protects the deployment of DRM systems, while in Article 5.2(b) it mandates private copying levies for analog and digital equipment and media. What 5.2(b) says is that insofar as Member States permit private copying, they should provide for fair compensation, i.e. levies, to the right owners. The amount of fair compensation, however, should "take account of the application or non-application for technological measures." The idea behind this rather opaque language is that if you would not take into account the deployment of DRM, consumers would end up paying twice: first to the rights owners, directly under the DRM system, and a second time indirectly through the levy system. So, to avoid such double payment, the Directive effectively sets out a track for the gradually phasing out of levies.

But what to make of that language in the Directive? How to "take account of the application or non-application of technological measures"? That's one of the many difficult questions that European lawmakers are facing today. Does it mean that national authorities are under an obligation to measure the actual degree of use of DRM systems? Does it mean they will have to measure what percentage of content actually is being protected by technological measures? And if so, what is the base line there? Should it be measured against a "perfect world" where 100% of content is securely delivered through DRM systems? And how should we measure that? If you think about it—and at our institute we have been thinking about it; we are actually finalizing a study which tries to make sense of this provision—you quickly come to the conclusion that this is not doable. This simply doesn't work. So, you have to look at other alternatives to give at least some meaning to this phasing out of levies. What we have come up with, a reading based on the recitals preceding the Directive, is that we should not look at actual degrees of usage, because that is an immeasurable and hopeless task. Instead we should look at the actual availability of DRM systems in the marketplace—availability, not simply as a function of the state of technology, but also in terms of economic viability. What are costs for content distributors, what are the costs for consumers, and particularly to what extent will consumers actually accept these technological measures, these DRM systems? In this respect, the very interesting discussion of yesterday afternoon will play a crucial role: what may consumers reasonably expect from DRM?

Last but not least, we should look at the legal side of the coin. Are there technological measures available in the marketplace that comply

with the law? Do they sufficiently respect privacy in such a way that the main reason for introducing levies in the first place, which was to protect the user's privacy, has disappeared? What all this adds up to is a process of technology assessment in a very broad sense, a regular (annual or bi-annual) rule-making procedure, to be conducted by the European Commission, national authorities or copyright tribunals. What it shows is that you might use the impending phase-out of levies as an incentive to introduce DRM systems that are socially acceptable. Until that happens, levies and DRM are bound to exist side by side for some time, as will, we all hope, "old Europe" and the United States. Thank you very much.

. . . .

QUESTIONER: FRITZ ATTAWAY, MOTION PICTURE ASSOCIATION OF AMERICA: A question for Professor Hugenholtz. Jack Valenti is frequently demonized for having suggesting back in the 1980s that levies be placed on VCRs. You may have heard that this morning. If this is such an absurd idea, why have so many of the world's great democracies in Europe adopted this ridiculous scheme?

HUGENHOLTZ: This is a trick question. I wasn't there when all of this happened, but I don't think if the choice had been between a prohibition on copying equipment and a levy, the choice would have been so difficult to make. But it all starts with imposing contributory liability. If that had not happened in Germany, I don't think we would have had levies in Europe.

LEMLEY: Let me just add one thing to that. You can look at a levy system in one of two ways, right? You might look at a levy system as a replacement for a copyright infringement system. That is, you can be sued for copyright infringement, but if instead you pay a tax that justifies the cost of the copying, then you can no longer be sued for copyright infringement, and your use is justified. Alternatively, you can look at a levy as a supplement to an existing system of copyright infringement, in which you say you will pay a tax and you will still be prohibited from making copies that violate the copyright law under the tax. It seems to me that how one feels about levies might differ greatly depending on what system a particular individual has in mind.

QUESTIONER, DON WHITESIDE, INTEL CORP.: I am curious what your view is of the efficiency of the levies infrastructure. The objective clearly is to provide compensation, and fair compensation, back to the rights holder; and I am curious what your perspective is on how the money is collected, whether the rates are done through a formal process, and how much of those funds actually make it back to the rights holders.

HUGENHOLTZ: There's indeed very little transparency in the way many levy systems operate in Europe. Tariffs are more or less randomly set, sometimes in negotiations between collecting societies and equipment or media manufacturers, sometimes ordained by government authorities or copyright tribunals. The transparency further decreases as you look downstream. The way levies are being redistributed, or "repartitioned" as they say, by the large collective societies to rights holders is murky, to say the least. It is a very, very nontransparent process.

LEMLEY: All right, please join me in thanking the panel.