2003

DRM and Privacy

Julie E. Cohen
Georgetown University Law Center, jec@law.georgetown.edu

18 Berkeley Tech. L.J. 575-617 (2003)

DRM and Privacy

18 Berkeley Tech. L.J. 575-617 (2003)

Julie E. Cohen
Professor of Law
Georgetown University Law Center
jec@law.georgetown.edu

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 no-

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

---

tices from February through November 2002); U.S. FEDERAL TRADE COMM'N, WARRANTY 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.

at stake in decisions about privacy arguably are not an appropriate subject 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 statu-

---

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.

tory mandates.[78] Extending the full protection of the FIPs to all consumers 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

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. 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).

practices is broad enough to encompass such a move.[80] Put differently, a 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 indi-

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 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.

viduals retain meaningful control over both the spatial and informational dimensions of their own intellectual consumption.[85]

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

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.

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, Com-*

imperfections focuses on issues of market power. If a dominant vendor has 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

---

puters, 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.

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.

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.

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-

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

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/pollsandbehavior.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 pro-

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.

---

hibition 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. 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.

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. Arguments 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 differ-

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

ent 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, 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

---

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

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 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

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.

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.

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 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,

---

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).

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; 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

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.

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—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

---

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.

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, 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 participa-

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 Commit-

tion 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 grievances, 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]

---

tee); 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).

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).

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 intellectual 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.