Denver Law Review

Volume 84 | Issue 1 Article 8

January 2006

Beyond Copyright: Managing Information Rights with DRM

Viktor Mayer-Schonberger

Beyond Copyright: Managing Information Rights with DRM

BEYOND COPYRIGHT: MANAGING INFORMATION RIGHTS WITH DRM

VIKTOR MAYER-SCHÖNBERGER†

INTRODUCTION

For the first 150 years of United States copyright law the legal prohibition of unauthorized copying was aided by the technical limitations consumers faced when wanting to duplicate content. The Xerox machine made copying of paper-based content faster and less costly; so did the widespread availability of audiocassette and videotape recorders. Yet, as long as information remained stored in analog form, copying tended to result in a loss of quality. The copy of the copy of a music cassette lacks the fidelity of the original. To be sure, piracy existed even then, but it did not happen primarily at the consumer end of the value chain. Pirates generally required sophisticated and costly equipment and a functioning distribution channel. Over time, rights holders improved their ability to interdict pirates around the world.

Digital technology changed the historical status quo. Duplication technology enabled consumers to make perfect copies for a fraction of the cost and time. The Internet added a cheap and fast distribution channel with peer-to-peer software providing an unprecedented level of ease-of-use in downloading copyrighted content. Rapidly, illegal copying became much cheaper than doing so legally, leading to the widespread "sharing" of copyrighted information among consumers without rights holders' consent, thus—as rights holders contend—reducing market demand for the informational goods they offer.[1]

Rights holders see digital rights management (DRM) as a tool to rectify this situation using a double strategy. First, and much reported in the media, DRM aims at making illegal copying harder and more costly.[2] Second, often overlooked but at least of equal importance, DRM is in-

---

† Associate Professor of Public Policy, The John F. Kennedy School of Government, Harvard University. I gratefully acknowledge the research assistance of Malte Ziewitz and financial support from the Dean's Research Fund at the Kennedy School of Government.

1. *See* Press Release, Recording Indus. Ass'n of America, Music Industry Unveils New Business Strategies and Combats Piracy During 2002 (Feb. 28, 2003), *available at* http://www.riaa.com/news/newsletter/022803.asp (citing online piracy as a major cause of the 9% decline in CD shipments in 2002); *see also* Stephen Manes, *Full Disclosure: Copyright Law–Ignore it at your own Peril*, PC WORLD, Sept. 2003, *available at* http://www.pcworld.com/howto/article/0,aid,111657,00.asp. For an economic analysis, see Stan Liebowitz, *File-Sharing: Creative Destruction or Just Plain Destruction?*, 49 J.L. & ECON. 1, 17-18 (2006).

2. *See, e.g.*, Amy Harmon, *Pondering Value of Copyright vs. Innovation*, N.Y. TIMES, Mar. 3, 2003, at C2; Jeff Howe, *Licensed to Bill*, WIRED, Oct. 2001, at 140; John Markoff, *Five Giants in Technology Unite to Deter File Sharing*, N.Y. TIMES, Jan. 5, 2004, at C1.

tended to lower costs for obtaining content legally. The goal of DRM is to enable and facilitate legal licensing of digital information by reducing the transactional costs for consumers to find, access, and use the digital information they demand. Ease of use has propelled Apple's iTunes Music Store to become the preeminent legal music download site on the Internet, causing customers more than a billion times to say "yes" to "DRMed" music.[3]

Much of the debate over DRM so far has focused on these contested intellectual property issues, in particular on copyright.[4] However, copyright is not the only legal claim over information. Privacy rights, for example, entitle individuals to some control over their personal information.[5] DRM is generally agnostic as to what kinds of rights over information it protects and the transactions of what rights it facilitates, as long as such rights can be technically incorporated. This, in turn, requires one, at least at some level, to find common conceptual ground among such information rights.

This Article argues that DRM may prove useful beyond the narrow confines of copyright. Part I briefly describes DRM and why and how DRM can be used to manage rights over information more generally. Part II maps the elements of DRM systems, with a specific focus on the meta-data that defines specific usage rights of the DRMed information it accompanies. Part III looks at non-copyright claims over information, in particular informational privacy, and evaluates how such claims could be represented in DRM systems. I put forward a list of advantages such DRM-based management of informational privacy claims would offer and lay out three significant challenges and how they could be addressed for such a DRM system to be successful.

I. THE EMERGENCE OF DRM SYSTEMS

Digital rights management aims to control access to information content.[6] It does so by covering all phases of access control, from describing access rights to a certain piece of information, to facilitating transactions of such rights, to enforcing access control. While DRM comes in many different kinds and shapes, it needs to be comprehensive—covering all stages of the dissemination and usage process—to prevent content from being extracted from its protective realm by unauthorized parties.

---

3. Press Release, Apple Computer Inc., iTunes Music Store Downloads Top One Billion Songs (Feb. 23, 2006), *available at* http://www.apple.com/pr/library/2006/feb/23itms.html.

4. *See generally* Symposium, *Law and Technology of Digital Rights Management*, 18 BERKELEY TECH. L.J. 697 (2003); Nicola Lucchi, *Intellectual Property Rights in Digital Media*, 53 BUFF. L. REV. 1111 (2005).

5. *See, e.g.*, Julie Tuan, *Customer Information:* U.S. West, Inc. v. FCC, 15 BERKELEY TECH. L.J. 353, 368-69 (2000) (discussing the right to privacy as it relates to personal information).

6. Access control is limited to preventing unauthorized users from access. It also entails enabling access for those that are authorized. *See supra* notes 1-2 and accompanying text.

Movies stored on DVDs are a good example. Movie data is already encrypted when it is transferred on DVD. DVDs are sold with the information on it encrypted and thus only playable through specific hardware. These DVD players, in turn, must be able to decrypt the movie information. DVD production, DVDs and DVD players all have to conform to the same technical rules on how digital information is being interpreted for DRM to work, and all parties must adhere to these rules for the system to function.[7]

Such DRM requires a complex system of technical, organizational and societal elements. Neither technology nor market incentives alone will be sufficient, for at least two reasons.

First, many but not necessarily all commercial entities involved in the dissemination of DRMed content have a strong economic interest to ensure that the DRM system remains in place. Take the manufacturers of DVD players, for example. If they were to sell a DVD player that could "break" the DRM system and permit its users easy duplication of encrypted data—much like dual-deck music cassette recorders used to offer—consumers might buy more of these units, creating an economic incentive for manufacturers of DVD players to defect from the DRM system.[8]

Second, consumers will desire to "free ride," that is, to gain access to DRMed content without paying the appropriate usage fee. To that end, consumers will want to collect information and methods as well as tools to break the access control mechanisms of DRM unless societal rules prevent them from doing so.[9]

For DRM to work, therefore, the legal system has to stop defections by commercial entities as well as prevent consumers from gaining and sharing information about how to break usage restrictions, while enabling and facilitating authorized transactions of usage rights. What usage

---

7. The most important DRM standard for video DVDs is the "Content Scrambling System" (CSS), an authentication and encryption system designed to prevent unauthorized copying of DVDs. *See* JIM TAYLOR, DVD DEMYSTIFIED 481-85 (2d ed. 2001). This system was hacked in 1999 by software called DeCSS. *See* Rob Pegoraro, *Hollywood to Home Viewer: We Own You*, WASH. POST, Aug. 25, 2000, at E01. For the elaborate next generation of content protection systems, see, for example, the High-Definition Multimedia Interface (HDMI), an industry-supported standard to connect any compatible digital audio or video source like a Sony Playstation and a video recorder, and the respective DRM standard High-Bandwidth Digital Content Protection (HDCP), a lack of which may lead to video quality and resolution being artificially downgraded. *See generally* Digital Content Protection, LLC, http://www.digital-cp.com/home (last visited Sept. 14, 2006). Another example is Apple's DRM technology FairPlay, which restricts access to digital content on Apple's products, such as iTunes or the iPod. *See* Hiawatha Bray, *Apple's Music Operation Hits a Sour Note*, BOSTON GLOBE, Aug. 2, 2004, at C2.

8. *See* TAYLOR, *supra* note 7, at 481 (citing the corollary proposition that DVD producers are not willing to publish DVDs without protection from DRM defecting practices).

9. *See* Pegoraro, *supra* note 7, at E01 (citing at least one instance where users have illegally hacked a DVD encryption system); *see also* Bill Rosenblatt, *iTunes DRM Hacked, Then Hacked Again*, DRM WATCH, Mar. 24, 2005, http://www.drmwatch.com/drmtech/article.php/3492676 (discussing hacking of Apple, Inc.'s FairPlay DRM).

rights, however, are being granted through DRM, no longer need to be a simple reflection of the legal system. In fact, one can imagine a DRM system granting its users a very different set of rights than current intellectual property law—especially when compared with fair use rights.[10]

As Lawrence Lessig predicted, the authority to delimit these usage rights shifts from the existing lawmaking and adjudicating institutions in our society to those in control of the DRM system.[11] The law's task in such a context is to ensure that such private ordering is not being undermined by "leakage" and circumvention.[12] Thus, intellectual property law turns into an enforcement mechanism for whatever access control arrangements are contained in DRM.

Critics have contended that every DRM system to date has been broken relatively swiftly, eroding the very foundation on which the entire idea of access control rests.[13] However, enforcement does not need to be perfect—it is sufficient if it deters enough to shape the behavior of many consumers.[14] Apple's DRM is a case in point: The use of music bought through the iTunes Music Store online and downloaded onto one's computer is constrained by a system called FairPlay.[15] It restricts the computer on which the music can be played, the iPod onto which it can be copied, and how often it can be burnt on a CD. To break out of this straight-jacket, many tools have been developed and remain available on the Internet to either strip the music from FairPlay restriction data, or to otherwise enable the unauthorized sharing of DRMed music content.

---

10. For an early comparison between intellectual property law and the DRM system envisioned by Ted Nelson's famous System Xanadu, *see* Pamela Samuelson & Robert J. Glushko, *Intellectual Property Rights for Digital Library and Hypertext Publishing Systems*, 6 HARV. J.L. & TECH. 237, 239, 247-52 (1993).

11. *See generally* LAWRENCE LESSIG, CODE AND OTHER LAWS IN CYBERSPACE (1999); *see also* Viktor Mayer-Schönberger, *In Search of the Story: Narratives of Intellectual Property*, 10 VA. J.L. & TECH. 11, para. 36-40 (2005); Joel R. Reidenberg, *Lex Informatica: The Formulation of Information Policy Rules Through Technology*, 76 TEX. L. REV. 553, 591-92 (1998); VIKTOR MAYER-SCHÖNBERGER, DAS RECHT AM INFO-HIGHWAY 41 (1997).

12. *See generally* ROBERT C. ELLICKSON, ORDER WITHOUT LAW: HOW NEIGHBORS SETTLE DISPUTES (1991); *see also* Yochai Benkler, *An Unhurried View of Private Ordering in Information Transactions*, 53 VAND. L. REV. 2063, 2078 (2000); Lawrence Friedman, *Essay: Digital Communications Technology and New Possibilities for Private Ordering*, 9 ROGER WILLIAMS U. L. REV. 57, 61-62 (2003); David R. Johnson & David G. Post, *And How Shall the Net Be Governed?: A Meditation on the Relative Virtues of Decentralized, Emergent Law*, *in* COORDINATING THE INTERNET 62, 81-90 (Brian Kahin & James H. Keller eds., 1997); Margaret Jane Radin & R. Polk Wagner, *The Myth of Private Ordering: Discovering Legal Realism in Cyberspace*, 73 CHI.-KENT L. REV. 1295 (1998).

13. *See, e.g.*, John Black, *The Impossibility of Technology-Based DRM and a Modest Suggestion*, 3 J. ON TELECOMM. & HIGH TECH. L. 387, 396 (2005) (arguing that "the media companies' reliance on a technological solution is almost certainly doomed, and that a variety of motives will continue to drive people to circumvent any such technology. The best solution to the problem is not a technological one, but instead one of education.").

14. *See* Viktor Mayer-Schönberger, *The Shape of Governance: Analyzing the World of Internet Regulation*, 43 VA. J. INT'L L. 605, 614-16 (2003); *see also* Jack L. Goldsmith, *Regulation of the Internet: Three Persistent Fallacies*, 73 CHI.-KENT L. REV. 1119, 1126 (1998); Lawrence Lessig, *The Zones of Cyberspace*, 48 STAN. L. REV. 1403, 1405 (1996).

15. *See* Bray, *supra* note 7, at C2.

Creating, disseminating and using such tools may be potentially illegal, but nevertheless continues to take place. This has not doomed Apple's DRM system. Despite the widespread availability of such tools at low transactional costs and the persistence of music sharing peer-to-peer networks, consumers buy DRMed music from the iTunes Music Store at a rate of about four million usage restricted songs per week.[16] Consumers are obviously willing to pay a relatively small amount in return for ease of use, speed of search and download, and assurance of quality.

Less than perfect DRM systems will continue to thrive as long as content owners deem the revenue generated more important than the leakages of content that are occurring. Of course, any change in the value proposition to the consumer—for example by raising prices or making pricing less transparent—may have an effect on consumer behavior, potentially increasing leakage and undermining the DRM system. This is one reason Apple has a strong incentive to keep iTunes Music Store's pricing model simple and transparent.[17]

DRM is more than a technical fix to prevent unauthorized copying. As a system, it depends not just on technology, but on institutions and market incentives, and presupposes law to prevent too much leakage from happening. While not perfect, DRM systems have been relatively successful in controlling access and will remain so as long as their value propositions are attractive. Insofar as DRM systems prescribe acceptable usage behavior, they replace the legal system as the dominant normative framework.

II. ELEMENTS OF DRM SYSTEMS AND IMPLICATIONS

In abstract terms, a DRM system consists of both mechanisms for facilitating authorized transactions and mechanisms for enforcing access control. The former covers functions like the publishing of DRMed content, the easy searching for content by consumers, and the processing of the transaction itself. This may include the creation and management of online directory services as well as electronic payment.[18] The latter en-

16. Press Release, Apple Computers Inc., iTunes Music Store Downloads Top 150 Million Songs (Oct. 14, 2004), *available at* http://www.apple.com/pr/library/2004/oct/14itunes.html.

17. The recent clash between Apple and the big music labels over pricing strategies can be seen against the backdrop of this conflict. *See* Scott Morrison, *Labels Demand a Bite as Apple Calls the Tune*, FIN. TIMES (London), Mar. 4, 2005, at 11 (citing the music labels' concerns that wholesale prices should be raised to capture a larger share of the market in which they believe Apple has become too powerful).

18. *See* Niels Rump, *Definition, Aspects, and Overview*, *in* DIGITAL RIGHTS MANAGEMENT: TECHNOLOGICAL, ECONOMIC, LEGAL AND POLITICAL ASPECTS 3-4 (Eberhard Becker et al. eds., 2003); *see also* Ahmad-Reza Sadeghi & Markus Schneider, *Electronic Payment Systems*, *in* DIGITAL RIGHTS MANAGEMENT: TECHNOLOGICAL, ECONOMIC, LEGAL AND POLITICAL ASPECTS 113-115 (Eberhard Becker et al. eds., 2003).

tails mostly technical means to restrict usage of content to certain users, times, and modes.[19]

Both facilitating transactions and enforcing access control require the DRM system to authenticate users as well as content, and to incorporate and respect usage data associated with the specific content users have acquired.[20] The need for authentication has been well documented and linked to debates on electronic signatures and similar methods of authenticating messages.[21] The role of usage data—information about how a particular content may be used—has received less attention although such meta-data is a fundamental element of DRM.[22]

To perform its role of controlling access, any DRM system must "know" what kind of usage is permissible by whom, and what usage attempts must be prevented. This is done through meta-data associated with content that describes authorized usage.[23] If a consumer attempts to use content in a way that contradicts the usage rights expressed in the meta-data, the DRM system will attempt to stop her. Consequently, a DRM system needs to know how to locate such meta-data for any DRMed content it manages, and most current DRM systems rely on content to contain or be combined with the relevant meta-data.

Meta-data has to lay out permissible use in a standardized and unambiguous way, so that it can be used by all technical elements of a DRM system. In recent years, two major attempts got under way to systematically define meta-data for a very wide spectrum of digital content. The first one is eXtensible Rights Markup Language (XrML) developed and owned by commercial entity ContentGuard and based on the "extensible markup language" (XML).[24] Microsoft employs a version of XrML in the DRM it uses.[25]

---

19. *See* Rump, *supra* note 18, at 30-42.

20. There is significant philosophical debate among DRM providers whether to authenticate users or usage devices. Most DRM systems discussed in this paper focus on user authentication, but the Digital Media Project (DMP) instead focuses on device authentication. *See* Bill Rosenblatt, *2005 Year in Review: DRM Standards*, DRM WATCH, Jan. 2, 2006, http://www.drmwatch.com/standards/article.php/3574511.

21. *See generally* LESSIG, *supra* note 11, at 30-42; L. JEAN CAMP, TRUST AND RISK IN INTERNET COMMERCE 36-40 (2000) (pointing to the difficulties of evaluating the reliability of information online); DAVID BRIN, THE TRANSPARENT SOCIETY 179-81, 333-35 (1998) (arguing that in view of modern surveillance technologies, we should focus more on ensuring accountability, i.e. reciprocal transparency, than protecting privacy by fostering secrecy).

22. *See* Stefan Bechtold, *Digital Rights Management in the United States and Europe*, 52 AM. J. COMP. L. 323, 326-29 (2004).

23. Already more than a decade ago and way ahead of the time, Pam Samuelson and Bob Glushko wrote eloquently about the need for such meta-data and its implications. *See* Samuelson & Glushko, *supra* note 10, at 252-53.

24. Andrew Conry-Murray, *XrML: Defining Digital Rights*, IT ARCHITECT, Apr. 5, 2004 http://www.itarchitect.com/shared/article/showArticle.jhtml?articleId=18900094.

25. *See* Stacy Cowley & Paul Roberts, *Microsoft Details Rights Management Policy*, NETWORK WORLD, Feb. 21, 2003, http://www.networkworld.com/news/2003/0221microdetai2.html

Another derivative of XrML is REL, a "rights expression language" that is part of the MPEG-21 standard.[26] By adopting REL, the Moving Picture Experts Group (MPEG) hopes that it will aid in the creation of a comprehensive DRM for multimedia content.[27] REL in turn uses standardized terms in describing the usage rights for specific content. These terms are defined in what is called the Rights Data Dictionary (RDD) that is being developed under guidance of the International Standardization Organization (ISO).[28]

The RDD, developed by UK-based firm Rightscom Ltd,[29] defines the terms rights holders can use when creating usage meta-data that defines who can do what, with which resource, in what context, at what time, and in what location. Accordingly, RDD contains semantics for defining agents, resource, time, place and context (in RDD parlance the "context model").[30]

While impressive in its structured approach, XrML's long-term sustainability in the market place is an open question. After years of use Microsoft's version of XrML remains incompatible with MPEG's REL; and the software giant has no apparent plans to change this. REL on the other hand has not seen a single implementation by any of the many industry players that initially praised it, prompting experts to call it "irrelevant."[31]

The second attempt to standardize meta-data is the Open Digital Rights Language (ODRL) Initiative, orchestrated by its founder Renato Iannella.[32] ODRL covers the same ground as XrML. Unlike XrML, however, ODRL stems from an open process and is offered license-free. It is the open-source pendant to commercial XrML. Not surprisingly, ODRL has collaborated with Creative Commons (CC)[33] to map CC's semantics in ODRL.[34]

(citing John Manferdelli, general manager of the Windows Trusted Platform Technologies group: "Despite being new, XrML is the richest and best developed of the rights management languages.").

26. *See* Rosenblatt, *supra* note 20.

27. *See* Rightscom Ltd, *The MPEG-21 Rights Expression Language* 5 (July 14, 2003) (White Paper), *available at* , http://www.interactivemusicnetwork.org/documenti/view_document.php?file_id=809.

28. *See* Rosenblatt, *supra* note 20.

29. Rightscom, http://www.rightscom.com/Default.aspx?tabid=1076 (last visited Sept. 14, 2006).

30. *See* Susanne Guth, *Rights Expression Languages*, *in* DIGITAL RIGHTS MANAGEMENT: TECHNOLOGICAL, ECONOMIC, LEGAL AND POLITICAL ASPECTS 101, 103-105 (Eberhard Becker et al. eds., 2003).

31. *See* Rosenblatt, *supra* note 20.

32. The Open Digital Rights Language Initiative, http://odrl.net (last visited Sept. 14, 2006).

33. Creative Commons is a non-profit organization that offers flexible copyright licenses for creative works. *See* Creative Commons, http://creativecommons.org/ (last visited Sept. 14, 2006).

34. *See* ODRL Creative Commons Profile, July 6, 2005, http://odrl.net/Profiles/CC/SPEC-20050706.html.

ODRL has been successfully used in the area of mobile devices, where the Open Mobile Alliance (OMA) has adopted it for its DRM, leading to widespread use in mobile devices in Europe.[35] North American operators on the other hand have so far chosen mostly to use their own proprietary DRM systems.[36]

ODRL's biggest immediate challenge is not technical or economic, but legal. In what can only be described as a second-order intellectual property war, ContentGuard, the company that developed XrML, maintains that its patents cover any implementation of a rights expression language and has threatened open, royalty-free ODRL.[37] ODRL's proponents maintain that ContentGuard's wide-reaching patent claims are baseless.[38] Yet, the legal question of who holds intellectual property rights over the way by which we may semantically describe intellectual property claims in DRM remains unresolved, thus clouding considerably ODRL's future.[39]

Neither XrML nor ODRL are likely to become the accepted standard for expressing usage rights in DRM systems any time soon. Not only does each of them have their own problems, they also have to contend with a growing plethora of proprietary DRM systems advocated by commercial competitors as well as industry consortia.[40] The lack of interoperability between these systems, the high economic stakes involved, and the entrenchment of leading players—rights holders, consumer electronics corporations, telecommunication companies and software producers—will continue to work against widespread consolidation.[41]

To sum up, DRM systems consist of a number of important elements to perform two main functions—the facilitation of usage rights transactions, and the interdiction of unauthorized use. A central element is the representation of usage rights in the DRM system. It is often achieved by specifying such rights through a distinct rights expression

---

35. *See* Rosenblatt, *supra* note 20; Open Mobile Alliance, *Digital Rights Management* 4 (Dec. 2003) (Short Paper), *available at* http://www.openmobilealliance.org/docs/DRM%20Short%20Paper%20DEC%202003%20.pdf; Open Mobile Alliance, Press Release, The Open Mobile Alliance Shows Growing Industry Impact 1-2 (Oct. 20, 2005), *available at* http://www.openmobilealliance.org/docs/AGM2005RlsFINAL.pdf.

36. *See* Rosenblatt, *supra* note 20 ("OMA DRM is taking hold primarily in Europe; the standard's loss of momentum is jeopardizing its chances for adoption across the Pond in North America.").

37. *Id.* ("One reason for the OMA DRM slowdown has been the still-unresolved wrangling over DRM patent licensing terms . . . .").

38. *See* Susanne Guth & Renato Iannella, *Critical Review of MPEG LA Software Patent Claims*, INDICARE, Mar. 23, 2005, http://www.indicare.org/tiki-read_article.php?articleId=90 (questioning the validity of ContentGuard's patents).

39. *See id.* ("If the claims of MPEG LA are validated, the work of the ODRL Initiative and other RELs such as the Creative Commons Licenses will be critically endangered.").

40. *See* Rosenblatt, *supra* note 20 (mentioning a number of other proprietary standards like Groovy Mobile and Melodeo in the U.S. and Canada or Cingular's cooperation with Apple's FairPlay DRM in Motorola cell phones).

41. *See id.*

language with semantics pre-defined in a (potentially extensible) dictionary. Two significant efforts for defining such a rights expression language have been undertaken recently—the commercial XrML/REL and open source license-free ODRL, but neither will likely become the dominant standard in the medium term, nor will any of the available alternatives. The lack of a common standard, however, does not put in dispute the central need to represent usage rights in DRM.

III. REPRESENTING RIGHTS IN DRM

To date, DRM systems are used to control access to copyrighted information content, be it movies, video games, software or music. Technically, these different types of content are all the same: streams of bits, with associated meta-data that restrict what can be done with them. As DRM systems are built to control access to "digital" information, they are fundamentally rights agnostic—that is, they can in principle restrict any digital bit stream.

Hence, one could potentially extend such DRM systems to intellectual property rights beyond copyright.[42] For example, one could envision trademark rights to be managed through DRM. If one were to use a trademarked name or image, the DRM system could facilitate the licensing of such trademarks or prevent their use. Widening the scope of rights management in such a way would require, however, a significant modification of the semantics of usage. So far, these semantics—as evidenced for example by the Rights Data Dictionary (RDD)—focus on simple uses of managed content, like printing, displaying, storing or modifying.[43] Including trademark rights in DRM would necessitate deepening the "understanding" that the DRM system has of the context of use: Is the trademark just mentioned descriptively, or does its use infringe upon the rights of the trademark holder? Answering this question may require machines to understand substantially more about the substance of information than is currently available. Yet, in a number of instances existing DRM systems may easily be able to protect trademark rights, just as they protect copyrights. Take for example the use of logos on web pages: in such cases the DRM could require (and facilitate) the user to obtain consent from the trademark owner. To be sure, this would not stop somebody from scanning in a trademarked logo and then using it, but it would arguably prevent a user from downloading a trademarked logo from the trademark owner's website to use the same logo on her website, even if the logo itself were not copyrighted.

---

42. Although, perhaps with the exception of trademark rights, it is a bit hard to imagine what these other intellectual property rights could be. Simply put, unlike copyright, patent rights protect product or process ideas, not just concrete instantiations of these ideas. Thus, it is hard to see what bit stream a DRM intent upon protecting patents rights would control and how.

43. *See* Rosenblatt, *supra* note 20.

Intellectual property is but one right over information our legal system recognizes. DRM systems could potentially be used to manage other rights over information. Given how much we expose personal information on the Internet and the extent to which this exposure is abused, one obvious candidate for such an extension could be informational privacy—the management and protection of personal information.

A. Advantages of DRM-Based Protection of Personal Privacy

At least at first blush, such protection of informational privacy through a DRM system seems to be a useful idea for a number of reasons.

First, the Internet has made processes less transparent. With complex information processing in our computers, protecting personal information is less obvious to users than before. A DRM system would take care of this complexity of information flows for users—providing users with options without exposing them to the underlying complexity.

Second, due to the abundance and affordability of digital processing and storage, we capture, process and store much more information about ourselves—from photos and movies to financial transactions – compared with pre-digital times with its specialized equipment and relatively expensive storage costs, thereby increasing the footprint of our individual digital shadows.[44] With DRM built into all devices that acquire, store and process information, this surge in stored information of personal character would not necessarily translate into an equal increase in personal vulnerability.

Third, even without our expressed wish, information processing equipment we use—from personal computers to cell phones—acquire and store much more information about our interactions than ever before—much of which may represent personal information to which we would like to control access.[45] A DRM system would enable us to do so.

---

44. *See, e.g.*, Chip Walter, *Kryder's Law*, SCIENTIFIC AM., Aug. 2005, *available at* http://www.sciam.com/article.cfm?articleID=000B0C22-0805-12D8-BDFD83414B7F0000&ref=sciam (arguing that Moore's law about "the doubling of processor speed every 18 months is a snail's pace compared with rising hard-disk capacity" and stating that "[s]ince the introduction of the disk drive in 1956, the density of information it can record has swelled from a paltry 2,000 bits to 100 billion bits (gigabits), all crowded in the small space of a square inch.").

45. A recent victim of this lack of control over one's personal information has been socialite Paris Hilton, whose cell phone was allegedly hacked. *See* John Schwartz, *Some Sympathy for Paris Hilton*, N.Y. TIMES, Feb. 27, 2005, § 4, at 1. More generally, malware, spyware, hacking, and other attacks on communications devices has dramatically increased over the last couple of years – including the hundreds of thousands of computers in the U.S. alone that are hijacked and remote-controlled from abroad. *See, e.g.*, CERT/CC Statistics 1988-2006, http://www.cert.org/stats/ (last visited Sept. 14, 2006) (stating that the number of reported attacks against internet-connected systems has increased from 21,756 in 2000 to 137,529 in 2003). For a more detailed analysis, see Jonathan L. Zittrain, *The Generative Internet*, 119 HARV. L. REV. 1974, 2008-13 (2006).

Fourth, the original thrust of protecting personal information in the United States stemmed from the fears of a "Big Brother"-like, overarching (federal) government.[46] Born out of the shadow of the Watergate scandal, the Federal Privacy Act[47] therefore protects citizens from intrusion by the federal government.[48] At least since the advent of the Internet and electronic commerce, consumers have come to realize that commercial entities may threaten their privacy just like governments. In contrast to the European privacy landscape, U.S. federal legislators so far have not enacted an omnibus data protection statute that covers the private sector as well.[49] A DRM system could address this problem by empowering people to control access to their personal information regardless of whether the party attempting such access is a government agency or a commercial entity.

Fifth, unlike copyright laws that have been harmonized around the world through a century of international treaties, informational privacy statutes, despite some international coordination like the OECD Guidelines on the Protection of Personal Data, have not seen a similar harmonization.[50] In particular, in the United States, informational privacy rights remain a patchwork of state and federal laws, making it possible for personal information to be exported with the help of the Internet to a jurisdiction with less stringent privacy laws.[51] This leads to legal arbi-

46. *See* COLIN J. BENNETT, REGULATING PRIVACY – DATA PROTECTION AND PUBLIC POLICY IN EUROPE AND THE UNITED STATES vii (1992); DAVID H. FLAHERTY, PROTECTING PRIVACY IN SURVEILLANCE SOCIETIES – THE FEDERAL REPUBLIC OF GERMANY, SWEDEN, FRANCE, CANADA, AND THE UNITED STATES xiii (1989); Viktor Mayer-Schönberger, *Generational Development of Data Protection in Europe*, *in* TECHNOLOGY AND PRIVACY: THE NEW LANDSCAPE 219, 221 (Philip E. Agre & Marc Rotenberg eds., 1997).

47. Federal Privacy Act, 5 U.S.C.A. § 552a (West 2006).

48. *See* PAUL M. SCHWARTZ & JOEL R. REIDENBERG, DATA PRIVACY LAW 92 (1996) ("The Privacy Act represents the most comprehensive attempt to structure information processing within the public sector.").

49. There are, however, a number of rather specific sectoral omnibus data protection statutes, such as the Video Rental Record Protection Act (18 U.S.C.A. § 2710 (West 2006)), the Drivers Privacy Protection Act (18 U.S.C.A. §§ 2721-25 (West 2006)), the Health Insurance Portability and Accountability Act (42 U.S.C.A. §§ 1320d, 1320d-1 – 1320d-8 (West 2006)), or the Right to Financial Privacy Act (12 U.S.C.A. §§ 3401-3403 (West 2006)). *See also* SCHWARTZ & REIDENBERG, *supra* note 48, at 215-18 (giving a brief overview of data protection in the private sector in the U.S.).

50. Organization for Co-Operation and Economic Development (OECD), *OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data*, http://www.oecd.org/document/18/0,2340,en_2649_34255_1815186_1_1_1_1,00.html (last visited Sept. 14, 2006). Harmonization has therefore taken place to a certain degree. However, in the European Union this was largely due to the European Union Data Protection Directive. *See* EU Directive 95/46/EC on the Protection of Individuals with Regard to the Processing of Personal Data and on the Free Movement of such Data, Oct. 24, 1995, *available at* http://ec.europa.eu/justice_home/fsj/privacy/law/index_en.htm [hereinafter Data Directive].

51. While there is no comprehensive and homogeneous body of privacy law at the federal level in the U.S., informational privacy is protected to varying degrees by rather diverse state laws. *See* SCHWARTZ & REIDENBERG, *supra* note 48, at 129-30 ("[N]o two states have adopted precisely the same system of regulation."). This is one of the reasons why the European communities linked the export of personal data to third countries to the requirement of a certain minimum level of protection. *See* Data Directive Art. 25, *supra* note 50 ("The Member States shall provide that the transfer to a third country of personal data which are undergoing processing or are intended for processing after transfer may take place only if, without prejudice to compliance with the national provi-

trage—a modern form of "forum shopping."[52] A DRM system would have global reach and work largely independently of the jurisdiction it is being used in, thereby overcoming the arbitrage problem.[53]

Sixth, and related, entrusting a DRM system to protect our informational privacy would not necessitate the passage of a comprehensive digital privacy law, which legislative priorities as well as federalism concerns in the United States may preclude. As DRM relies on law to stop leakages from occurring too frequently, a relatively simple amendment to the Digital Millennium Copyright Act (DMCA)[54] prohibiting tampering with DRM systems in general (and not just in the context of intellectual property rights) could suffice.

Because of the potential of DRM systems to address these privacy challenges, DRMing personal information may possibly offer all of us better individual control over our personal information than current privacy law does.

B. Three Challenges to DRMing Informational Privacy

To achieve success, however, at least three issues exist—one technical, one foundational, and one conceptual—that may prevent us from using DRM in the personal privacy context.

1. The Technical Challenge

As I have described above, DRM systems depend on meta-data of permissible use that is linked to the content to which the meta-data refers.[55] This linkage has to be hard to break, because once separation happens, content essentially loses its protective cover and can no longer be protected by DRM. A number of technical methods are used by DRM systems to ensure the linkage between (as well as the integrity of) meta-data and content. For example, meta-data can be "embedded" in content,

---

sions adopted pursuant to the other provisions of this Directive, the third country in question ensures an adequate level of protection."). Subsequently, an EU delegation negotiated with the U.S. Department of Commerce the so-called safe-harbor principles. *See* U.S. Department of Commerce, Safe Harbor, http://www.export.gov/safeharbor/index.html (last visited Sept. 14, 2006).

52. *See* A. Michael Froomkin, *The Internet as a Source of Regulatory Arbitrage*, *in* BORDERS IN CYBERSPACE 129, 140-50 (Brian Kahin & Charles Nesson eds., 1997); Viktor Mayer-Schönberger, *The Shape of Governance: Analyzing the World of Internet Regulation*, 43 VA. J. INT'L L. 605, 615 (2003); *see also* Joel Trachtman, *Cyberspace, Sovereignty, Jurisdiction, and Modernism*, 5 IND. J. GLOBAL LEGAL STUD. 561, 577 (1998) ("One dark side of cyberspace is its facilitation of private sector jurisdictional evasion and, at least in some contexts, its facilitation of regulatory arbitrage."); Sean Selin, Comment, *Governing Cyberspace: The Need for an International Solution*, 32 GONZ. L. REV. 365, 381-82 (1996) (speaking of the "lowest common denominator" that would result in such regulatory arbitrage).

53. To be sure, as I have mentioned above, technology requires laws to prohibit the creation and use of tools to break technological locks. In the absence of supportive laws one could overcome the restrictions the DRM system imposes without breaking the law. However, even in these situations, one could imagine contract law to take over some of the role of the (inexistent) laws.

54. Digital Millennium Copyright Act § 103, 17 U.S.C.A. § 1201 (West 2006).

55. *See supra* text accompanying notes 20-28.

using mechanisms like steganography[56] and encryption.[57] As a rule of thumb, employing these methods is easier when the amount of meta-data is relatively small compared with the content that needs to be protected. This is the case with multimillion-pixel photographs, megabyte-sized music files, or videos measured in gigabytes.

Unfortunately, personal information is much smaller. Our social security number is only nine digits in length, all of which are numbers. In such cases the meta-data defining permissible usage would be substantially bigger than the informational content it intends to protect, requiring DRM system builders to fundamentally adjust their systems, while steganography and similar methods of "hiding" and "embedding" meta-data would have to be replaced by more robust mechanisms that work without depending on a relative size difference between meta-data and protected content.

Yet, providers of DRM systems may have to face this challenge regardless of whether we want to include personal information or not. As digital creators continue to combine and modify pre-existing elements to build new works, the notion of the individual creator producing a monolithic creative work is rapidly substituted by ideas of peer production, John Seely Brown's creative bricolages, and a modus operandi of "rip, mix, and burn."[58] Providers of DRM systems will have to contend with this brave new world of intellectual production, in which individual creative elements that are assembled, combined, and mixed, may get smaller and smaller in size. If that is the case, the problem of linking smaller pieces of information with its meta-data that I have described above may get solved anyway.

2. The Foundational Challenge

For a DRM system to be comprehensive and effective in managing personal information rights it needs to keep track of what users are doing when, how, and in what context.[59] Consequently, in order to protect the privacy of individuals, a DRM system needs to keep track of everybody's every move, thus creating a system of total surveillance.

---

56. Steganography is "the act of embedding or hiding a message inside a seemingly innocent digital vessel" so that nobody except for the recipient knows of its existence. *See* J. William Gurley, *From Wired to Wiretapped: Forget Privacy Rights. The Real Problem With Government Net Snooping is That it Won't Work*, FORTUNE, Oct. 15, 2001, at 214.

57. *See* SIMSON GARFINKEL & GENE SPAFFORD, WEB SECURITY AND COMMERCE 187-208 (Deborah Russel ed., 1997) (referring to the process of converting a plaintext message into a supposedly unintelligible ciphertext by using an encryption algorithm, i.e. a mathematical equation).

58. For a comprehensive analysis of social production as a new paradigm, see generally YOCHAI BENKLER, THE WEALTH OF NETWORKS: HOW SOCIAL PRODUCTION TRANSFORMS MARKETS AND FREEDOM (2006).

59. *See generally* Richard Gooch, *Requirements for DRM Systems*, *in* DIGITAL RIGHTS MANAGEMENT: TECHNOLOGICAL, ECONOMIC, LEGAL AND POLITICAL ASPECTS 16 (Eberhard Becker et al. eds., 2003) (providing a general overview of the requirements of an effective DRM system).

Inherent in this perplexing situation is the notion that such DRM systems need to be tracking comprehensively in order to be effective.[60] Yet, as I have discussed above, DRM systems do not need to offer perfect, but only sufficient enforcement.[61] Limited leakage is not detrimental as long as most individuals continue to choose transacting through DRM rather than circumventing it.

The problem of leakage, however, might become more difficult the smaller and more fluid the informational content DRM intends to protect. Leakage of a multi-gigabyte movie file may be less troublesome, because distributing such a file at current transmission speeds carries non-trivial transactional costs.[62] Such costs are practically non-existent for a piece of personal information that just contains a person's name and social security number. Sending and receiving such information across the Internet takes milliseconds. Therefore, one could argue that the smaller the information pieces DRM systems have to protect, the more comprehensive such systems must become.

Yet, such a view presupposes that transaction costs stay constant. The more bandwidth users will have at their disposal, the lower the transaction costs for transferring even large pieces of information. As providers of DRM will adapt their systems to a high bandwidth world, for example by building the capacity to "forget" into our digital systems, such leakage could be controlled effectively.

3. The Conceptual Challenge

Existing DRM systems incorporate a semantic of property. This is not surprising considering that they are designed to protect copyright. The dictionaries they employ—for example the RDD—are based on property-related actions, like "sell." The legal foundation of informational privacy claims, on the other hand, is based on a negative liberty, a right to keep others out.[63] It is not conceptualized in terms of permission and licensing, of selling and transacting rights to others.

---

60. *See id.*

61. *See id.*

62. *See id.*

63. *See, e.g.*, Samuel D. Warren & Louis D. Brandeis, *The Right to Privacy*, 4 HARV. L. REV. 193, 193 (1890) (the seminal article that became the basis of the right to privacy in the U.S.). Legal academics have argued since for different notions of privacy. Charles Fried equates informational privacy with control over information. *See* Charles Fried, *Privacy*, 77 YALE L.J. 475, 483 (1968). Paul Schwartz argued for a concept based on informational self-determination. *See* Paul M. Schwartz, *Privacy and Democracy in Cyberspace*, 52 VAND. L. REV. 1609, 1653 (1999). Julie Cohen suggested individual autonomy as a foundation for privacy. *See* Julie E. Cohen, *Examined Lives: Informational Privacy and the Subject as Object*, 52 STAN. L. REV. 1373, 1423 (2000). Both Schwartz's and Cohen's approach are instantiations of essentially European, if not German notions of informational privacy. *See* Spiros Simitis, *Reviewing Privacy in an Information Society*, 135 U. PA. L. REV. 707 (1987); Mayer-Schönberger, *supra* note 46, at 229-32. Categorizing these and similar conceptions of informational privacy, Daniel Solove has identified six main themes: the right to be let alone, limited access to self, secrecy, informational control, personhood, and intimacy. *See*

This results in a mismatch between the semantics available in current DRM systems and the conception of the claim—informational privacy—we intend to incorporate. There are two options to overcome this divergence.

First, one could adjust our conception of informational privacy to conform to the property paradigm already built into DRM systems; that is one could change the law to fit the technology. As long as the relation between humans and information can be represented in terms of ownership and property, such "propertized" informational privacy claims could be included in existing DRM systems.

"Propertizing" information privacy is not a novel idea. Experts from Kenneth Laudon to Lawrence Lessig have suggested it before.[64] They argue that while our legal system has not conceived of informational privacy as a property right, markets have. Personal information has become a valuable commodity that is traded once it has been collected. Hence, using property as a legal foundation for informational privacy would arguably bring the legal system in line with economic reality, with the benefit of empowering the original source of personal information—the individual herself. Such "propertization" of personal information could then provide the conceptual foundation that enables DRM systems to manage access to such information, thereby potentially—as Lessig contends—enabling the individual to decide whether and to what extent to trade away her privacy interests in personal information.[65]

Yet, as has been pointed out, such a reconceptualization of informational privacy is not without significant problems.[66] First, copyright and patent rights are granted to offer an individual economic incentive for the production of creative works to overcome potential underproduction of

---

Daniel J. Solove, *Conceptualizing Privacy*, 90 CAL. L. REV. 1087, 1094 (2002). None of these privacy conceptions, however, is founded on a property paradigm similar to copyright.

64. *See* Kenneth C. Laudon, *Markets and Privacy*, 39 COMM. OF THE ACM 92 (1996); LESSIG, *supra* note 11, at 122-134; Lawrence Lessig, *The Architecture of Privacy*, 1 VAND. J. ENT. L. & PRAC. 56, 58 (1999); *see also* Patricia Mell, *Seeking Shade in a Land of Perpetual Sunlight: Privacy as Property in the Electronic Wilderness*, 11 BERKELEY TECH. L.J. 1, 26-41 (1996); Richard S. Murphy, *Property Rights in Personal Information: An Economic Defense of Privacy*, 84 GEO. L.J. 2381, 2381 (1996); Edward Janger, *Privacy Property, Information Costs, and the Anticommons*, 54 HASTINGS L.J. 899, 900 (2003); Jerry Kang & Benedikt Buchner, *Privacy in Atlantis*, 18 HARV. J.L. & TECH. 230, 267 (2004); Paul M. Schwartz, *Property, Privacy, and Personal Data*, 117 HARV. L. REV. 2055, 2058 (2004).

65. *See* LESSIG, *supra* note 11, at 156-62. *But see* Andrew Orlowski, *Lessig, Stallman on "Open Source" DRM*, THE REGISTER, Apr. 15, 2006, at 1, *available at* http://www.theregister.co.uk/2006/04/15/lessig_stallman_drm.

66. *See* Pamela Samuelson, *Privacy as Intellectual Property?*, 52 STAN. L. REV. 1125, 1136-46 (2000); Marc Rotenberg, *Fair Information Practices and the Architecture of Privacy (What Larry Doesn't Get)*, 2001 STAN. TECH. L. REV. 1, § 2 (2001); Rochelle Cooper Dreyfuss, *Warren & Brandeis Redux: Finding (More) Privacy Protection in Intellectual Property Lore*, 1999 STAN. TECH. L. REV. 8, 12; Jerry Kang, *Information Privacy in Cyberspace Transactions*, 50 STAN. L. REV. 1193, 1193 (1998); Janger, *supra* note 64, at 914-16.

such works.[67] This is different for personal information, which arguably is not underproduced.[68] Second, intellectual property laws in the United States are designed, as the Constitution states in unambiguous terms, to advance the public good through the advancement of science and the arts.[69] There is no such utilitarian rationale in facilitating the dissemination of personal information.[70] Third, propertization is anathema to those that conceptualize informational privacy in terms of individual autonomy and dignity.[71] Fourth, certain uses of a creative work after its copyright had been sold may infuriate the creator, but unlike personal information will not threaten her *persona*.[72]

Moreover, our traditional notion of creative works is atomistic: Creative works stand on their own; they may shape (at least in part) the context they are put in, not vice versa. For example, one can read a Shakespeare play, or a Beckett novel on the beach, in the subway, or in a library—it, we assume, rises above the context in which it is read. Consequently, in most cases creators have little interest in dictating where we consume their creations. This is different in the realm of personal information. The use of personal information in one context may be perfectly benign and acceptable to the individual the information refers to, but use in a different context may have serious negative consequences for that person.[73] Through the act of propertization, the originator loses control of her personal information and cannot stop it from being used by others who have legitimately obtained "ownership" rights over it.

---

67. *See* WILLIAM M. LANDES & RICHARD A. POSNER, THE ECONOMIC STRUCTURE OF INTELLECTUAL PROPERTY LAW 13 (2003).

68. *See* Kang, *supra* note 66, at 1193 n.237; *see also* Murphy, *supra* note 64, at 2383; *see also* Samuelson, *supra* note 66, at 1139.

69. U.S. CONST. art 1, § 8 (stipulating that "Congress shall have power . . . to promote the progress of science and useful arts, by securing for limited times to author and inventors the exclusive right to their respective writings and discoveries.").

70. *See* Samuelson, *supra* note 66, at 1140-41.

71. *See* Kang & Buchner, *supra* note 64, at 234-36; *see also* Samuelson, *supra* note 66, at 1142-43.

72. *See* Rotenberg, *supra* note 66, at § 93 (noting that Warren & Brandeis in their seminal paper on privacy "purposefully distinguished a privacy right from an intellectual property claim, noting that copyright typically protects an interest once publication occurs, privacy protects a right to simply not publish"); *see also* Samuelson, *supra* note 66, at 1138 (stating "[f]ree alienability works very well in the market for automobiles and land, but it is far from clear that it will work well for information privacy. An individual may be willing to sell his data to company N for purpose S, but he may not wish to give N rights to sell these data to M").

73. An extreme example is offered by the development in the 1930s in the Netherlands of a comprehensive population registration system. The objective of the system echoes some of the rationales for more sophisticated information technologies today—to streamline administration and to reduce burdens on citizens. That system, however, was subsequently used to assist the Nazis in apprehending Dutch Jews and Gypsies, who suffered a much higher death rate than any other occupied western European country, or, notably, Jewish refugees in the Netherlands, who were not in the registration system. *See* William Seltzer & Margo Anderson, *The Dark Side of Numbers: The Role of Population Data Systems in Human Rights Abuses*, 68 SOCIAL RESEARCH 2 (2001); *see also* David Lazer & Viktor Mayer-Schönberger, *Statutory Frameworks for Regulating Information Flows: Drawing Lessons for the DNA Data Banks from other Government Data Systems*, 34 J.L. MED. & ETHICS 366, 368 (2006).

Proponents of DRMing personal information may rebut that the dangers of de- and re-contextualization are not unique to personal information. In fact, they could argue, the more we tend to combine, modify and adapt creative works in digital bricolages, the less such creative works are able to evoke their own individual context. Creators consequently will desire to retain more control over the contexts in which their creative works are being used, moving away from the property notion underlying current DRM systems. In turn, this may force DRM systems to augment their underlying structure of usage rights to include context—granted a very tall order, given the current state of technologies.

A second, possibly more sensible option is the reverse; to make technology follow the law, by altering DRM systems to include non-property based concepts. This is relatively straightforward as long as it can be achieved by adjusting the semantics of rights expressed in DRM. Relevant dictionaries, like the RDD, would be modified, thereby making way for the inclusion of informational privacy into DRM systems. Yet, it is uncertain that such a simple semantic "patch" can be sufficient, for the concept of property not only rests on semantics, but on how we construe the relations between humans and information. In a property framework, such a relation is constructed in terms of a subject/object relationship of exclusive ownership and control. If, however, our conception of informational privacy is built on an alternative conceptualization of the linkage between humans and information, if, to quote Julie Cohen's words, in informational privacy the "subject" is the "object,"[74] a simple semantic modification of DRM is no longer feasible.

This is not to suggest that Cohen's conception of informational privacy is the most appropriate one. Rather, it is precisely the absence of a prevalent conception of informational privacy—unlike the property-inspired orthodoxy of copyright—that makes it so difficult to adjust DRM systems to. If we fail to agree on a conception of the right we want to protect, how can we hope to express this conception in code, i.e. in standardized, relatively unambiguous language? And even if we had such an agreed-upon conception of informational privacy we would have to incorporate it into a DRM system in addition to the conception of copyright that is already mapped in our DRM systems. How would these two presumably very different conceptions coexist? Would such a DRM system use one common or two separate dictionaries expressing the various elements of usage rights and relations between user, rights holder, and information?

The obvious, but conceptually complex solution, of course, is to suggest a common structure of rights over information that is able to represent a variety of different rights over information, from copyright to

74. Cohen, *supra* note 63, at 1373.

privacy.[75] Given the pitfalls of other solutions, investing serious thought into conceptualizing such a common structure seems the most promising long-term solution.

CONCLUSION

This article examined DRM systems and their capacity to manage not just copyrights but also other kinds of rights over information. In particular, I looked at whether, to what extent and under what conditions informational privacy rights could be managed through DRM. I discussed a number of advantages of DRMing informational privacy rights, and presented three significant challenges to its adoption—a technical, a foundational, and a conceptual one—and suggested possible paths to address them.

While these hurdles are significant and it is not clear whether and when they can be cleared, it is in the DRM system providers' best interest to broaden the scope of the systems they use, not only because it widens the market, but also because empowering individuals to better manage their informational privacy rights may in turn bring about a public reassessment of the value DRM systems offer.

75. Finding such common ground may be easier in the continental European context. *See* VIKTOR MAYER-SCHÖNBERGER, INFORMATION UND RECHT (2001).