

INFUSING PRIVACY NORMS IN DRM

Incentives and perspectives from law

ALEX CAMERON

LL.M. (Law and Technology) Candidate, University of Ottawa, Canada

Abstract: This paper outlines some basic characteristics of digital rights management (DRM) systems, as well as the ways that DRM systems can threaten user privacy. The author asserts that consent-based privacy laws are alone insufficient to address privacy threats posed by DRM. The author suggests that privacy norms can be infused in DRM design and implementation and that the interests of end-users, DRM engineers and DRM users support striving toward that goal.

Key words: Digital rights management, copyright, privacy, law, legal aspects.

It is a commonplace that the characteristic virtue of Englishmen is their power of sustained practical activity, and their characteristic vice a reluctance to test the quality of that activity by reference to principles. [...] Most generations, it might be said, walk in a path which they neither make nor discover, but accept; the main thing is that they should march. The blinkers worn by Englishmen enable them to trot all the more steadily along the beaten road, without being disturbed by curiosity as to their destination.

R.H. Tawney, 1921¹

It seems that engineers and lawyers do not talk to one another enough these days. Driven by the copyright industries and with the blinkers of those industries in place, digital rights management technology is rapidly marching toward copyright owners' utopia of near-perfect control over copyright works. At the same time, driven by the concerns of citizens around the world, lawmakers in many countries are marching toward increased protection of privacy. Soon, these two marches will certainly collide.²⁻⁴

This paper explores the collision course between DRM and user privacy. Part 1 provides a brief overview of DRM technology and some incentives for its widespread implementation. Part 2 sketches some of varied ways that DRM systems can threaten user privacy. Part 3 asserts that consent-based privacy laws are alone insufficient to address the privacy threats posed by DRM. Finally, Part 4 argues that privacy norms can be infused in DRM design and implementation and that the interests of end-users, DRM engineers and DRM users support striving toward that goal.

1. FRAMEWORK FOR THINKING ABOUT DRM

An open digital networked environment presents a number of challenges for creators and distributors of literary, musical and other works. Although such works are typically protected under existing copyright laws, technology has dramatically increased the difficulty of enforcing those copyrights. Once a work is published, it can usually be copied perfectly and distributed widely without the permission of the owner and often in violation of their legal rights. The most well-known examples of this kind of problem are P2P file-sharing systems.

In response to these new challenges, owners of copyright works have started using DRM systems to level the playing field and to exploit the distribution opportunities that the networked environment offers them. While a detailed review of DRM technologies is unnecessary for the purposes of this paper, it is important to have a general understanding of how DRM works and what factors are motivating its uptake.ⁱ

1.1 Basic DRM functionality

DRM systems typically travel with copyright works and function like electronic security guards to monitor and control access and use of those works wherever they go. DRM is a form of persistent protection that is tied to works. The following definition of DRM used at a recent IASTED conference captures most of the key concepts:

[DRM] means the chain of hardware and software services and technologies governing the authorized use of digital content and management of any consequences of that use throughout the entire life cycle of the content. DRM is an access and copy control system for digital content, such that the DRM securely conveys and enforces

ⁱ There are a number of published articles which conduct detailed reviews of DRM technology.⁵⁻⁷

complex usage rights rather than simple low-level access/copy controls. [...] DRM technologies include a range of functions to support the management of intellectual property for digital resources, such as expression of rights offers and agreements, description, identification, trading, protection, monitoring and tracking of digital content.⁸

In relation to the works that they protect, DRM systems are usually categorized by whether they function to control access, use, or both. Many perform both functions and many utilize a number of different technologies in doing so.⁴⁻⁷

DRM systems can also be used to automatically *enforce* legal or contractual rights in relation to works. With DRM, copyright owners are no longer required to enforce their copyrights using the jurisdiction-limited, expensive and time-consuming legal system – by way of licenses with each user, they can efficiently replace the rules of copyright law with their own privately-written and -enforced rules.⁹ For example, if a particular user is permitted (for a fee) to listen to a DRM-protected song three times over a 12 hour period but instead tries to listen once and copy part of it, then the DRM system might, among other things, automatically delete the work from the user's computer (assuming the license with the user allowed for that).

Finally, as suggested by the definition above, DRM systems often contain surveillance and reporting functionality which allow copyright owners to track access and use of their works or to single out and profile the activities of particular users. These DRM functions directly implicate user privacy and will be discussed further in Part 2 of this paper.

1.2 Factors motivating DRM

In the basic ways described above, DRM systems promise copyright owners inexpensive, automated and near-perfect control over works of all kinds. If a user does not agree to the owner's rules (which will almost always include payment of a fee), then the user will not be permitted to access or make use of a work. Put another way, DRM allows copyright owners to restrict and in many cases foreclose the possibility of copyright infringement from ever happening.

The copyright industries tell us that their protective technologies are a response to widespread copyright infringement. That is the premise upon which they have lobbied governments to implement legal protections for DRM technology. It is also the premise upon which, for example, the United States passed such legal protections in the controversial *Digital Millennium Copyright Act*.¹⁰ In very general terms, the *DMCA* makes it illegal to circumvent DRM systems or to develop technologies which circumvent DRM. There is no question that DRM is designed to protect against

copyright infringement. However, the real promise of DRM and likely the single biggest incentive for its adoption goes far beyond responding to new forms of copyright infringement.

Early in the history of DRM development, Barlow eloquently expressed the idea that DRM would transform “a market where wine is sold in bottles from which everyone may drink infinitely—as is the case with books—into a market where all wine is sold by the sip. Forever.”¹¹ His vision is as true today as it was in 1998. The copyright industries are keenly interested in DRM because it allows them to exploit every conceivable use of a work,ⁱⁱ including “paid downloads, subscriptions, pay-per-view and pay-per-listen, usage metering, peer-to-peer, superdistribution, and selling rights instead of the actual content.”¹² In a world where DRM systems are pervasive, copyright owners’ imagination is the only limit to their ability to exploit content; Stross predicts: “You might be able to read a library book... but your computer will be counting the words you read and monitoring your pulse so that it can bill you for the excitement it has delivered.”¹³

DRM promises copyright owners the ability to accomplish through private agreements with users what they cannot accomplish under copyright law.ⁱⁱⁱ Even the content that can be exploited using DRM need not be content to which any legal rights attach. DRM can be used to regulate the flow and use of virtually any type of information. To the extent DRM systems can deliver on these promises, they are poised to become the ubiquitous regulators of our ability to access and use copyright works and many other types of information.

2. DRM IMPLICATES PRIVACY RIGHTS

Although there is a growing body of legal and technical literature dealing with the issue, the privacy implications of DRM have not received the careful attention they deserve in light of the potential for a pervasive uptake of DRM. In fact, DRM systems pose a significant threat to user privacy because the fundamental premise of DRM is one of user identification and authentication. In other words, the principle job of a DRM system is to regulate who has permission to access and use a work.

By its very nature, DRM functionality requires users to disclose personal information to content providers.^{4,15} This information might include their

ⁱⁱ DRM may also allow users to purchase only what they really want (*e.g.* one song) rather than a larger package (*e.g.* a whole album). DRM also allows copyright owners to benefit from profiling users as described in Part 2.

ⁱⁱⁱ For example, DRM can allow for an indefinite term of protection. This issue places DRM in direct conflict with copyright concepts of fair use and public domain.¹⁴

name, email address, age, sex, mailing address, and credit card information. A DRM system would also normally require a user to designate a particular computer from which they will access and use the works; licenses are typically not transferable across different machines. User information must then be tied to a user profile in the DRM system which manages the rights that the user has in relation to various works. Given that DRM systems collect personal information about users in these ways virtually by necessity, there are at least three ways that DRM systems can implicate user privacy.

First, as an integral part of rights management and enforcement functions, many DRM systems will track and report on user activities – owners can use DRM systems “[to] stay in closer contact with their customers.”¹⁶ For example, each time a user requests access or use of a work, the request might be granted only after the identity and request of the user (or device) are verified against the user information database in the DRM system. At these periodic points of interaction between the user and the owner (or distributor), the system may automatically create a record of the interactions. Going one step further, the DRM system might surreptitiously monitor the work or user and report back to the owner regardless of whether or not the user does anything with the rights they have purchased. For example, a DRM system might periodically report back to the owner that the user has not done anything with a purchased work.

Tracking and recording DRM-gathered user information has a deep and broad impact on user privacy. Like other surveillance technologies, monitoring and recording user activities using DRM invades privacy because it interferes with intellectual freedom. Even when a user might not mind others knowing that they accessed or read certain content (which will usually be a very significant privacy concern), the user might not want others to know that they had to read it 20 times, that they highlighted parts of it, that they wrote notes in the margin, that they copied part of it, that they forwarded certain excerpts to their friends with comments, or that all of that cost them a bundle. For many users, knowledge that these or similar kinds of information would be gathered about them would naturally affect the types of content they choose to access and use, as well as how they go about it.^{iv} Cohen is particularly troubled by this invasion and argues that intellectual exploration is “one of the most personal and private of activities” and that in the invasion, DRM will “create records of behavior within private spaces, spaces within which one might reasonably expect that one’s behavior is not subject to observation.”²

Closely related to its monitoring and reporting capabilities, DRM poses a second threat to privacy because of its capability to profile users. Either by

^{iv} The important effects of surveillance on the behavior of individuals have been discussed at greater length in a number of articles.^{2,3,17}

using user information directly or by exporting user information to another system, DRM systems have the potential to create very detailed profiles about users' reading, listening, and watching activities and to tie that information to other information about them.^{15,18}

Beyond the *mere potential* for monitoring, recording and profiling, users should have every reason to expect that content owners will exploit those capabilities in DRM. At least in the case of larger commercial copyright owners, owners have a "compelling interest to monitor how purchased works are being used."¹⁸ At a high level, it makes perfect sense that profiling will occur because DRM is motivated by a desire to exploit every conceivable use of a work. With more data about discrete uses served up by DRM, copyright owners and others will simply have more information to feed into and better develop consumer profiling systems already in general use. Detailed and previously unavailable information about how users behave will have significant independent economic value for owners and others. In addition to processing user information for marketing or other purposes, DRM might allow owners to engage in sophisticated user-specific price discrimination.^{15,19}

The third privacy threat posed by DRM is perhaps the least obvious and most novel. To the extent that DRM involves controls over our ability to use works, Cohen argues that DRM has significant privacy implications:

Technologies that force changes in user behavior narrow the zone of freedom traditionally enjoyed for activities in private spaces and activities relating to intellectual consumption. In doing so, they decrease the level of autonomy that users enjoy with respect to the terms of use and enjoyment of intellectual goods.²

As Cohen acknowledges, this threat of control requires us to rethink "the nature of privacy and what counts, or ought to count, as privacy invasion in the age of networked digital technologies."² However, as DRM continues its ubiquitous march, this kind of "rethinking" about the nature of privacy may be necessary in order to ensure that we have spaces left within which to experience a right of privacy.

3. CONSENT-BASED PRIVACY LAWS AND DRM

Consent is the cornerstone of many if not most privacy regimes around the world.²⁰⁻²³ Many privacy laws and guidelines include provisions which require organizations to, for example, limit their collection of personal information to information that is necessary for identified purposes.^{21,24} In those kinds of provisions, the law presumes that individuals would not

consent to information collected for unidentified purposes or beyond what is necessary. Other provisions require organizations to obtain individuals' express consent before they process personal information. Where adequate user consent is obtained, it will usually be a sufficient justification for virtually any processing of personal information.

Thus, privacy regulation is largely premised upon the scope, nature and efficacy of the right of consent provided to individuals – the right to decide whether to consent to the collection and processing of their personal information. It is one of the key rights granted to individuals and it is also one of the key ways that organizations justify their processing of personal information. Consent is a big part of where privacy battles will be won or lost. These features of consent-based privacy laws are important because digital networked environments generally, and DRM systems in particular, cast serious doubt on the efficacy of consent as enabling meaningful privacy regulation.

DRM systems will usually require individuals to consent to some processing of personal information, usually by way of a clickwrap license agreement which incorporates a privacy clause. However, individuals often do not read these agreements which describe what they are consenting to, or even if they do read them, they do not or cannot understand the terms.^v A law professor, masters' student and law student recently studied several DRM-based content delivery services and came to the following conclusion:

The ways that information is collected and processed during use of the services examined is almost impenetrably complex. It is difficult to determine exactly what data a service collects, and merely discovering that separate monitoring entities sit behind the services requires a careful reading of the services' privacy policies.¹⁸

It is also important to note that when content is licensed using DRM, on a case-by-case basis users do not have any say about the owners' privacy terms. The choice typically presented to consumers in a standard form clickwrap license is "I agree" or "Cancel". There is no room for negotiation – no consent to the owner's privacy terms means no access to content. If individuals' privacy interests outweigh their desire to access DRM-protected content, then the market might help drive privacy-friendly DRM. On the other hand, to the extent that users agree *en masse* to owners' privacy terms (because they want access to DRM-protected content), DRM has the potential to rewrite privacy law in owners' terms in the same way it stands to rewrite copyright law. Privacy rights would then be dissolved into contract.

^v This problem has several facets. Privacy policies may sometimes be too general or they may be too detailed. There are also special considerations regarding consent in the electronic environment.²⁵

Some privacy regimes include provisions which may help address some of the problems posed by DRM systems. For example, some laws have provisions which restrict the ability of data collectors to make user consent a condition of providing wares or services.^{21,22} Other privacy rules require a high threshold for obtaining valid consent; for example, the *Directive on data processing* requires “unambiguous”²⁰ consent and the *Directive on electronic commerce* mandates that certain prescribed information must be conveyed “clearly, comprehensively and unambiguously” to electronic commerce consumers.²⁶ In the United Kingdom²² and Canada,²¹ the nature of the consent required for processing data is also tied in part to the nature of the information at issue – the more sensitive the information, the more explicit the consent must be.

If respected, these kinds of provisions will help give meaning and effect to the right of consent. Yet, short of more invasive and paternalistic privacy regulation (which can have ramifications of its own as described in Part 4), the law is limited in its ability to remedy the problems posed by DRM so long as it is jurisdiction-limited, difficult to enforce and divorced from the design and implementation of the very technology that threatens it.

4. A ROLE FOR PRIVACY NORMS IN DRM

While using technology to address legal problems rooted in technology is not a novel concept,²⁷ the following sub-sections attempt to go modestly further. The first briefly discusses existing proposals for achieving privacy-regarding DRM. The second sub-section sketches some of the diverse justifications for why it is in the interests of end-users, DRM engineers and DRM users to strive toward that goal.

4.1 Infusing privacy norms in DRM

With varying degrees of specificity, a number of authors in both law and engineering have suggested ways that privacy norms might be infused into DRM design and implementation. These range from merely raising the privacy question during design²⁸ to detailed descriptions of how to design DRM to act as “Privacy Rights Management” systems.²⁹

Drawing on inter-disciplinary research into technology design, Cohen advocates for a “value-centered” design process for DRM in which privacy would form part of the bundle of values driving DRM design.² Going one step further, Cohen argues that privacy law ought to help ensure that privacy is addressed in the process of setting DRM standards, a process which is currently underway. Perhaps as some indication of the soundness of Cohen’s

suggestion, but on the other side of the coin, it should be noted that a mandate of the Recording Industry Association of America is to “ensure that the protection of musical property rights is built into the relevant standards rather than added as an after-thought.”³⁰ Privacy laws already put forth a number of privacy values but there is limited evidence of those being reflected in DRM systems to date. What is clearly needed for the value-centered approach to be effective is for there to be a meaningful voice for privacy values at the standards-setting table.

Related to the “value-centered” design approach is the idea that privacy can be engineered into DRM through the consideration of privacy principles in the design process. Feigenbaum *et al.* suggest one such approach based on the OECD Guidelines; for example, they suggest that “[a] DRM system should provide easy pseudonymization that can be used to key databases.”³¹

The Information and Privacy Commissioner of Ontario published a practical step-by-step guide to injecting privacy into DRM.³² Aimed at DRM system developers and those who use DRM systems, this guide suggests implementing a system architecture (and code) which respects privacy rules, including “controls around the collection of personal information, linkability, access, use and accountability.” One of the interesting ideas mentioned in this guide and developed much further in other technical literature,²⁹ is the idea that DRM systems can be adapted to protect personal information in the same way that they protect copyright works. These *Privacy Rights Management* systems could offer individuals the same type of monitoring, access and use controls regarding their personal information that DRM systems offer to copyright owners. Using the language of DRM to draw a parallel, under a privacy rights management system individuals are the “owners” and their personal information is the “content”.

Notably absent from a number of the proposals described above, however, is a description of the means by which to address the consent-based issues described in Part 3 of this paper. Indeed, one of the proposals identified consent (or what the authors termed “choice”) as “one of the most difficult challenges.”³¹ One of the most interesting approaches to consent is an option-based approach; the following model was developed by Forrester Research:

At Level 1, visitors choose anonymity, deliberately forgoing the additional benefits offered by personalization and premium content. Retailers build trust by promising not to collect data or use cookies.

With the addition of convenient, targeted content or additional site access, consumers enter Level 2, a one-way communication relationship whereby merchants promise not to initiate contact with the shopper or disseminate personal information to third parties.

In Level 3, consumers agree to two-way communication with retailers. At this stage, visitors share more personally identifying information in exchange for proactive notifications of specials from the retailer. [...]

Level 4 is considered a trusting relationship, whereby shoppers seek advice and active solicitations from their merchants, including deals offered by established partners.³³

This multi-tiered approach presents a method by which businesses can develop trusting relationships with their customers. However, the approach also suggests that individuals will be able to make informed decisions about consent by choosing from a variety of options.³⁴ The very presentation of different options helps individuals understand what they are being asked when their consent is being sought. This is an approach which could be codified in DRM in order to help obtain consent that is unambiguous and informed.

4.2 Incentives for infusing privacy norms in DRM

Justifying a role for privacy law in DRM design and implementation is no easy feat. From the perspective of individual users and those who make and enforce privacy laws, there are no straightforward answers but a number of justifications are available. From the perspective of DRM engineers and DRM system users, the justifications are more nuanced and complex.

4.2.1 Users and lawmakers

On the whole, users and lawmakers would benefit by the infusion of privacy directly in DRM systems. With privacy rules embedded in DRM code, there should be less opportunity for privacy abuse and correspondingly less need for consumer concern about privacy and for actual legal enforcement of privacy rights. There is a serious risk, however, that governments and users may become irresponsible or complacent about privacy under the seemingly protective umbrella of privacy-infused DRM - they may incorrectly assume (to a degree) that code has supplanted law and is adequately addressing user privacy concerns.

Yet, in the same way that DRM may foreclose the possibility of copyright infringement from ever happening, so might it restrict or foreclose the possibility of privacy abuses occurring. For example, if a DRM system does not support surveillance of users, user privacy is likely better respected than if it were supported and the law restricted the practice, or worse, allowed it to occur with user consent. Or DRM might be adapted for use as *Privacy Rights Management*. All of this would be welcome news for users

and privacy regulators. Further, if users become more comfortable about their privacy in relation to DRM, then they may reap the benefits of increased DRM ecommerce activity, in the form of the lower prices that may follow such an increase.

Users might also benefit from privacy-infused DRM in the sense that they would incur less time and money costs adopting privacy enhancing technologies (PETs) or in defending against unwelcome marketing such as spam. Or users might be better off from a privacy perspective because they have not shown much interest in PETs, or in paying for PETs, in any event.

There are also a number of potential criticisms that might be directed against embedding privacy in DRM code. For one, the benefits described above assume that the law translates well into code and that the code is actually utilizing the best possible translation of the law. To the extent that the law does not translate well (because for example it includes subjective elements) or that the code does not accurately reflect the law for other reasons, infusing privacy in DRM may do a disservice to users' legal privacy rights.

There is equally a risk that even with relatively good privacy-infused DRM, the only privacy abuses that will be prevented by code are the clear-cut ones that happen infrequently in any event. The grey areas of abuse might go largely unchecked at the code level. This problem would be especially significant if governments and users became complacent about privacy as mentioned above.

These criticisms can be addressed in part by some of the proposals discussed in sub-section 4.1. For example, a DRM standard might require DRM systems to provide users or regulators some degree of access to its privacy architecture so that they can assess what privacy invasive and protective functions the system is actually capable of performing.

4.2.2 DRM engineers

The interests of DRM engineers are in some ways connected to the interests of DRM users because the latter group essentially pays the former to develop DRM systems. One might expect that this dynamic between DRM engineers and DRM users would discourage the infusion of privacy in DRM because DRM users' interests are assumed to typically militate against that. However, the dynamic may sometimes encourage the opposite result. Although DRM users might not have felt a significant squeeze yet, a number of other industries are increasingly feeling public and regulatory pressure to respect privacy. With laws allowing consumers rights of consent, access and the right to file privacy complaints, many businesses are incurring significant privacy compliance costs. This has caused some businesses to carefully

reconsider how much personal information they collect up-front in order to reduce potential downstream compliance costs. For others who choose to or must collect a lot of personal information, there is a strong incentive to make privacy compliance more efficient. Thus, DRM engineers who can deliver effective DRM that achieves the result on the privacy side should find a ready market for their products. In the long run, privacy-infused DRM products may also be less costly and more effective overall systems than those to which privacy is added as an after-thought.

There are also three ways that DRM engineers may have independent interests which support including privacy norms in DRM. First, there is an incentive for DRM engineers to produce privacy-infused DRM where a failure to do so would bring negative public or professional attention on them. This is particularly significant for DRM engineers who make more than just DRM products. Wanting to be (or wanting to appear to be) a good corporate citizen is a consideration which may encourage DRM engineers to infuse privacy considerations in DRM design independent of what DRM users may desire. Engineers' professional codes of conduct or ethics may also help encourage the development of privacy-regarding DRM.³⁶

A second incentive for DRM engineers to infuse privacy in DRM lies in the possibility that privacy abuses using DRM, if sufficiently serious or pervasive, may lead to the adoption of stronger privacy laws or stepped-up enforcement of current laws. This possibility and its effect on DRM users are discussed further in sub-section 4.2.3 below; the significance of this possibility for DRM engineers lies in the challenges that it may pose for innovation. In other words, stronger privacy laws created by lawmakers who probably do not understand engineers' work could directly interfere with engineers' ability to engage in innovative technological development.

The third way that DRM engineers might have an independent incentive to infuse privacy in DRM relates to the anti-circumvention provisions of the *DMCA* and similar legislation.^{vi} It is well-known that the *DMCA* has had a significant chilling effect on innovative technological research and development.³⁷ If DRM was infused with privacy, was widely accepted by end-users as a result and proved to be an effective distribution model, then there might be relatively little motivation for users to attempt to circumvent DRM protections. With little incentive to circumvent and little actual circumvention occurring, there would be less justification for *DMCA*-like legislation, particularly if DRM is pervasively adopted as a means of distribution. Although there are some lofty assumptions and tenuous causal links in this argument, what is suggested here is that undermining the justification for the *DMCA* in this way might help tip the scales to a repeal or

^{vi} Australia is the most recent country to agree to implement *DMCA*-like anti-circumvention legislation.³⁵

reform of the *DMCA*. This would be a welcome move for DRM engineers or others who find that their work is chilled by the *DMCA*'s current provisions.

4.2.3 DRM users

For the companies that use DRM systems, there are two key justifications motivating the infusion of privacy in DRM. The first relates to ecommerce uptake generally and the second relates to the potential for stronger privacy laws. A third possible incentive – relating to system cost, effectiveness and privacy compliance efficiency – was discussed above in sub-section 4.2.2.

If consumers believe that neither privacy law nor DRM technology do enough to protect privacy, then they may choose not to engage in ecommerce generally, and specifically they may choose not to purchase DRM-protected content. Businesses that use DRM systems are especially susceptible to this harm because of the potential for DRM to be used across many sectors and its potential to enable significant privacy violations. This is also an important concern for companies who enable DRM implementation and who provide the infrastructure for such commerce. There are therefore a broad range of pressures and incentives for DRM users to infuse privacy into DRM. Indeed, their survival may depend on it.

Closely related to the first justification, DRM users have an incentive to infuse privacy in their DRM systems in order to use their status as a selling feature, to gain a reputational advantage over competitors and to develop more trusting relationships with their customers.^{38,39}

The second key justification for infusing privacy in DRM stems from the likelihood that privacy laws or enforcement will be strengthened if there is a continued demand for privacy protection along with a failure in the market to protect privacy. A number of commentators^{40,41} have already sounded the alarm – they say that if immediate steps are not taken to protect privacy, then, like an endangered (if not already extinct) species, there may soon be no privacy left to protect. Although some might argue that it is too late to introduce intrusive legal regulation, it is arguable that more intrusive regulation might be a way of preventing the total destruction of privacy, or at least minimizing the risk of that happening. In the specific area of DRM technologies, there are several recent signs that such intrusive regulation may already be on its way.^{26,42,43}

To the extent that DRM systems are designed and implemented without regard for privacy, they may contribute to a consumer distrust of DRM, increased consumer privacy concerns generally and ultimately to stronger privacy laws or increased enforcement of current laws. Stronger privacy laws or enforcement efforts might even be specifically targeted at DRM systems or those who use such systems.^{26,42,43} In the short term, the two

consumer confidence factors will translate into losses for DRM users and related companies as mentioned at the outset of this sub-section. In the long term, if DRM users survive for very long, stronger or targeted privacy laws will only increase privacy risks and compliance costs for entities that use DRM. In these varied ways, infusing privacy in DRM design and implementation now ought to be a paramount concern for entities that use DRM.

5. CONCLUSION

In exploring the conflict between digital rights management and user privacy, my central objective is relatively modest. My aim is to commence a dialogue between engineers and lawyers, to prevent the solo marches of DRM systems and privacy legislations from a head-on collision. This paper has sketched some of the ways that DRM threatens privacy norms as well as the reasons why those threats cannot be adequately addressed by consent-based privacy laws alone. From the perspectives of three key DRM constituents, a case has been made here for the infusion of privacy norms in DRM design and implementation. That there are already detailed proposals setting out how that goal might be accomplished is a positive development. The issues discussed in this paper should provide useful incentives to implement one or more of those proposals, and to create and implement new ones.

ACKNOWLEDGEMENTS

The author wishes to thank to Dr. Ian Kerr, Canada Research Chair in Ethics, Law and Technology, for his personal encouragement and feedback in the preparation of this paper and for support through the inter-disciplinary research project of which he is Principle Investigator: “On the Identity Trail: Understanding the Importance and Impact of Anonymity and Authentication in a Networked Society” (www.anonequity.org). Thanks also to Vicky Laurens for sharing her insightful comments on an earlier draft.

REFERENCES

1. R.H. Tawney, *The Acquisitive Society* (G. Bell and Sons, London, 1921), p. 1.
2. J. Cohen, DRM and Privacy, 18 *Berkeley Tech. L.J.* 575 (2003).
3. J. Cohen, A Right to Read Anonymously: A Closer Look at “Copyright Management” in Cyberspace, 28 *Conn. L. Rev.* 981 (1996).

4. L.A. Bygrave, in: *Digital Rights Management - Technological, Economic, Legal and Political Aspects*, edited by E. Becker *et al.* (Springer, London, 2003).
5. I. Kerr, A. Maurushat, and C. Tacit, Technical Protection Measures: Part I - Trends in Technical Protection Measures and Circumvention Technologies (2003); http://www.pch.gc.ca/progs/ac-ca/progs/pda-cpb/pubs/protection/tdm_e.cfm.
6. European Commission, Digital Rights: Background, Systems Assessment, A Commission Staff Working Paper, submitted for discussion at a workshop in Brussels on February 28, 2002, on Digital Rights Management (February 2, 2002); http://europa.eu.int/information_society/newsroom/documents/drm_workingdoc.pdf.
7. European Committee for Standardization (CEN) and Information Society Standardization System, Digital Rights Management: Final Report (September 30, 2003); <http://europa.eu.int/comm/enterprise/ict/policy/doc/drm.pdf>, pp. 27-69.
8. M.I. Yagüe, IASTED International Conference on Communication, Network, and Information Security (2003); <http://www.iasted.com/conferences/2003/NewYork/cnis-specsess1.htm>.
9. L. Lessig, *Code and Other Laws of Cyberspace* (Basic Books, New York, 1999).
10. *Digital Millenium Copyright Act of 1998*, Pub. L. No. 105-304, 112 Stat. 2860 [DMCA].
11. J.P. Barlow, Life, Liberty and the Pursuit of Copyright? (September 17, 1998); <http://www.theatlantic.com/unbound/forum/copyright/barlow2.htm>.
12. B. Rosenblatt, B. Trippe, and S. Mooney, *Digital Rights Management: Business and Technology* (Hungry Minds/John Wiley, New York, 2001).
13. C. Stross, The Panopticon Singularity; <http://www.antipope.org/charlie/rant/panopticon-essay.html>.
14. D.L. Burk and J. Cohen, Fair Use Infrastructure for Rights Management Systems, 15 *Harv. J. Law & Tech.* 41 (2001).
15. Electronic Privacy Information Center (EPIC), Digital Rights Management and Privacy; <http://www.epic.org/privacy/drm/default.html>.
16. Microsoft Corporation, What is Windows Media DRM; <http://www.microsoft.com/windows/windowsmedia/WM7/DRM/what.aspx>.
17. J. Rosen, *The Unwanted Gaze: The Destruction of Privacy in America* (Random House, New York, 2000).
18. D.K. Mulligan, J. Han and A. J. Burstein, in: *Proceedings of the 2003 ACM workshop on Digital rights management* (ACM Press, New York, 2003), pp. 82-83.
19. A. Odlyzko, in: *Proceedings of the 5th international conference on Electronic commerce* (ACM Press, New York, 2003), pp. 355-366.
20. *Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data*, Official Journal L 281, 23/11/1995 pp. 0031-0050, Article 7(a) [Directive on data processing].
21. *Personal Information Protection and Electronic Documents Act*, S.C. 2000, c. 5, Schedule 1, Principle 4.3, 4.4, 4.3.3, 4.3.4 [PIPEDA].
22. *Data Protection Act 1998*, c.29, Schedule I - III.
23. *Federal Data Protection Act (Bundesdatenschutzgesetz)*, adopted 18 May 2001, published in the *Bundesgesetzblatt I Nr. 23/2001*, page 904 on 22 May 2001, section 4.
24. Organisation for Economic Co-operation and Development, *Guidelines on the Protection of Privacy and Transborder Flows of Personal Data* (OECD Publications, Paris, 2002), article 7 [OECD Guidelines].
25. V. Gautrais, The Color of E-consent, presented to the *Comparative IP & Cyberlaw Symposium at the University of Ottawa, October 2003*, forthcoming in 1 UOLTJ — (2004).

26. Directive 2000/31/EC of the European Parliament and of the Council of 8 June 2000 on certain legal aspects of information society services, in particular electronic commerce, in the Internal Market ('Directive on electronic commerce'), Official Journal L 178, 17/07/2000, pp. 0001-0016, Article 10.
27. B.L. Smith, The Third Industrial Revolution: Policymaking for the Internet, 3 *Colum. Sci. & Tech. L. Rev.* 1 (2001).
28. R. Dhamija and F. Wallenberg, in: *Proceedings of the First International Mobile IPR Workshop: Rights Management of Information Products on the Mobile Internet*, edited by O. Pitkänen (HIIT Publications, Helsinki, 2003), pp.13-23.
29. L. Korba and S. Kenny, in: *Security and Privacy in Digital Rights Management, ACM CCS-9 Workshop, DRM 2002, Washington, DC, USA, November 18, 2002, Revised Papers*, edited by J. Feigenbaum (Springer, London, 2003).
30. Recording Industry Association of America, Issues: New Media; <http://www.riaa.com/issues/audio/newmedia.asp>.
31. J. Feigenbaum, et al., in: *Revised Papers from the ACM CCS-8 Workshop on Security and Privacy in Digital Rights Management*, edited by T. Sander (Springer, London, 2001).
32. Information and Privacy Commissioner/Ontario, Privacy and Digital Rights Management (DRM): An Oxymoron? (October 2002); <http://www.ipc.on.ca/docs/drm.pdf>.
33. M. Pastore, Consumers Fear for Their Online Privacy (November 1, 1999); http://cyberatlas.internet.com/markets/retailing/article/0,,6061_228341,00.html.
34. J. Teh, Privacy Wars in Cyberspace: An Examination of the Legal and Business Tensions in Information Privacy, 4 *Yale J. of Law & Tech.* (2001-2002), p. 94.
35. Office of the United States Trade Representative, Free Trade 'Down Under': Summary of the U.S.-Australia Free Trade Agreement (February 8, 2004); <http://www.ustr.gov/releases/2004/02/2004-02-08-factsheet-australia.pdf>.
36. ACM/IEEE-CS, *Software Engineering Code of Ethics and Professional Practice, Version 5.2 as recommended by the ACM/IEEE-CS Joint Task Force on Software Engineering Ethics and Professional Practices and jointly approved by the ACM and the IEEE-CS as the standard for teaching and practicing software engineering* (1999); <http://www.acm.org/serving/se/code.htm#full>.
37. J.P. Liu, The DMCA and the Regulation of Scientific Research, 18 *Berkeley Tech. L.J.* 501 (2003).
38. A. Cavoukian et al., *The Privacy Payoff: How Successful Businesses Build Customer Trust* (McGraw Hill, Whitby, 2002).
39. D. Loukidelis, Thoughts on Private Sector Privacy Regulation (November 2003); http://www.oipcbc.org/publications/speeches_presentations/FIPAPIAspeech112403.pdf
40. B. Barr, A Tyrant's Toolbox: Technology and Privacy in America, 26 *J. Legis.* 71 (2000).
41. J. Cohen, Privacy, Ideology and Technology: A Response to Jeffrey Rosen, 89 *Geo. L.J.* 2029 (2001), p. 2035.
42. The Office of the Federal Privacy Commissioner (Australia), Media Release: No Sympathy for piracy or privacy bandits (November 20, 2003); http://www.privacy.gov.au/news/media/03_16.html.
43. *Consumers, Schools, and Libraries Digital Rights Management (DRM) Awareness Act of 2003*, S. 1621, 108th Cong. (2003).