

Digital Rights Management: Where Copyright and Privacy Collide

Alex Cameron*

Alex Cameron, *Digital Rights Management: Where Copyright and Privacy Collide* (2004) 2 C.P.L.R. 14.

Reprinted by permission of LexisNexis Canada Inc., from Canadian Privacy Law Review, edited by Michael Geist, Copyright 2004.

Copyright and privacy have come a long way together. When Warren and Brandeis embarked in their famous search for a right to privacy in 1890, they discussed the relationship between privacy, copyright law and the related independent right of authors to publish their works. More than a century later in our digital networked society, privacy is taking on increasing significance in the way that copyright issues are being resolved. It seems that privacy and copyright are increasingly colliding. Nowhere are these collisions greater than in the case of copyright industries' digital rights management (DRM) technology.

The modest aims of this article are threefold: to briefly introduce some of the recent conflict that has arisen between copyright and privacy, provide a basic overview of DRM technology and sketch DRM's privacy implications, including a short discussion of the *Personal Information and Electronic Documents Act* or PIPEDA. Increased awareness regarding the privacy implications of DRM is important given the potential for a pervasive uptake of DRM across many copyright and non-copyright sectors. For example, in the same way that DRM can protect and control copyright works as described below, DRM can be used by businesses to control access and use of sensitive documents or e-mails, including an ability to 'self-destruct' after a given time. Thinking about the privacy issues in DRM is also important because law may soon aggravate some of the privacy problems in DRM – in the context of Canada's copyright reform process, Canadian Heritage and Industry Canada are close to drafting new laws that will give legal protection to DRM.

Where Copyright and Privacy Collide

It is useful to begin with a reminder that the digital networked environment presents a number of opportunities and challenges for creators of literary, musical, dramatic

and other works. While these works are typically protected under national copyright laws, the networked environment has fundamentally changed the copyright landscape. Digitized works can be copied perfectly and infinitely and can be distributed globally at little or no cost.

Copyright industries are keen to exploit the unique opportunities that digital networks offer them. Yet, these same characteristics of digital networks are also a threat to copyright industries because their products can be easily copied and distributed without their knowledge or consent, including in ways that can be infringing. P2P file-sharing is probably the most widespread and well-known example of this kind of activity.

Copyright industries have responded to the opportunities and threats of digital networks in a number of ways, including through law and technology. In each of these areas, there are examples of copyright interests squarely colliding with privacy rights.

Among the legal responses, copyright industries around the world have initiated thousands of copyright infringement lawsuits against Web sites, on-line intermediaries and individuals. Privacy has played a starring role in a number of these cases where copyright industries have attempted to obtain personal information from Internet service providers (ISPs) about individual ISP subscribers.

In Canada and the United States, privacy rights have won the day in recent landmark rulings in *BMG Canada v. John Doe*¹ and *RIAA v. Verizon*.² In the *BMG Canada* case, which is currently under appeal, the Federal Court of Canada had to decide whether to order five Canadian ISPs to disclose the identity of 29 subscribers alleged to have committed copyright infringement. In refusing to order disclosure, the court criticized the recording industry's evidence and ruled that privacy considerations in the case outweighed the interest in pursuing the infringement lawsuits:

Without any evidence at all as to how IP address 24.84.179.98 has been traced to Geekboy@KaZaA, and without being satisfied that such evidence is reliable, it would be irresponsible for the Court to order the disclosure of the name of the account holder of IP address 24.84.179.98 and expose this individual to a law suit by the plaintiffs.

...

...given the age of the data, its unreliability and the serious possibility of an innocent account holder being identified, this Court is of the view that the privacy concerns outweigh the public interest concerns in favour of disclosure.

Despite refusing to order disclosure, the court was clear that privacy would not always trump copyright owners' interest in pursuing their lawsuits - the court left it open for the recording industry to come back to court with better evidence of the alleged wrongdoing. This case demonstrates that where copyright and privacy collide in Canadian courts, solid evidence of wrongdoing will likely be required before copyright will be permitted to trump privacy rights.

In addition to this type of legal response, copyright industries have pursued technological solutions to the opportunities and threats posed by digital networks. Prime among these solutions is DRM.

Overview of DRM Technology

In general terms, DRM is a form of persistent technological protection that travels with copyright works everywhere the works may go. DRM functions like an electronic security guard that monitors and controls access and use of works. Unlike a real security guard, DRM never leaves its post, never takes a break and never sleeps. Microsoft provides DRM solutions and defines DRM as follows:⁴

*DRM is a set of technologies content owners can use to protect their copyrights and **stay in closer contact with their customers**. In most instances, DRM is a system that encrypts digital media content and limits access to only those people who have acquired a proper licence to play the content. That is, DRM is a technology that enables the secure distribution, promotion, and sale of digital media content on the Internet.*
[Emphasis added.]

As stated in this definition, DRM often uses encryption technology to protect works. In fact, DRM is typically comprised of numerous technological components, including encryption, surveillance, a rights expression language, watermarking, digital signatures, fingerprinting, databases of works, owners and users and a licence management tool.⁵

Beyond simple copy-control mechanisms or password protections, most DRM is designed to automatically

establish and enforce potentially complex licence terms in relation to copyright works and other types of information. For example, a user might be permitted to read an article once for a fee under a DRM licence; if the user attempted to copy a portion of the article halfway through reading it, the DRM system might automatically delete the article if the licence included such a term. Thus, instead of having to engage inefficient legal mechanisms limited by geographic jurisdiction and the bounds of copyright law, with DRM copyright owners can write and automatically enforce their own rules in licences with each individual.

With its tight control over works, DRM aims to encourage authorized uses of copyright works by precluding infringement from ever happening at all. Beyond merely preventing infringement, however, copyright owners want to use DRM to deliver content because DRM allows owners to exploit every imaginable use of a work. With complete control over every access and use of a work, copyright owners' licensing opportunities are infinite. No longer will owners sell actual content to end-users. Instead, as has been happening in the software industry for years, owners will licence discrete rights to individuals to access or use content. Such licences might include any number of time, machine or use restrictions. We might then experience first-hand Barlow's vision of DRM transforming "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".⁶

DRM promises copyright owners a utopia of perpetual, automated and near-perfect control over their works. To the extent DRM can deliver on this promise, it is poised to become the ubiquitous regulator of our ability to access and use copyright works and virtually any other type of information product. In the non-copyright context, DRM may prove to be a valuable tool for businesses that wish to maintain control over important company information. In the copyright context, however, DRM has been criticized for placing excessive control in the hands of copyright owners, upsetting the balance in copyright law, locking up works in the public domain and denying the public's right to make fair use of copyright works. DRM can also have potential implications for privacy as discussed in the next section.

DRM and Privacy

It has probably become trite to assert that DRM implicates user privacy. The *EU Copyright Directive* codifies

recognition that DRM systems can have an impact on privacy where DRM processes data about consumption patterns and traces on-line behaviour. The *EU Copyright Directive* provides that DRM should be designed in accordance with the *EU Data Protection Directive*. The *Digital Millennium Copyright Act* in the United States permits circumvention of DRM for the protection of privacy. The Information and Privacy Commissioner of Ontario and reputed privacy groups such as the Electronic Privacy Information Center, have written on the issue, further confirming DRM's threats to privacy.⁷ While further study of DRM's impact on privacy is required, especially as new DRM systems and standards are developed, there is a growing body of literature addressing this important issue.

In basic terms, DRM developed to date can implicate privacy because its information collection and surveillance functions can provide copyright industries with highly detailed and previously unavailable information about the reading, listening and viewing habits of individuals. Each discrete access or use that an individual makes (or perhaps even attempts to make) in relation to a work can be recorded by a DRM system. For example, among many other things, copyright owners might be able to know how an individual paid for a movie on-line, how many times she watched it, whether she replayed any parts of it, whether she copied (or attempted to copy) all or part of it, and whether or not she sent (or tried to send) it to a friend.

The detailed information captured by DRM can then be used to construct fine-grained profiles of individuals, alone or by feeding into other surveillance or profiling systems in more general use. Even the emphasized portion of Microsoft's definition of DRM above hints at this potential.

In these ways, DRM can pose a serious threat to privacy because it collects information about each discrete access and use of the works it protects. Both the nature of this information and the level of its detail are unprecedented. Never before have copyright industries or others been able to obtain such information about what works users access and use (or attempt to access and use) and how, where, when and for how long such access or use occurs. In the world of tangible copyright works, individuals have not been subject to this kind of surveillance. For example, users can purchase a book or CD and do what they like with it in the privacy of their home on their own time. This is not the case with DRM-delivered works.

In addition to the nature and detail of the information collected by DRM, one of the most troubling aspects of

DRM's impact on privacy is the fact that DRM is collecting information while people are engaged in activities in places when and where they would likely have no expectation of being watched – DRM collects information while users are reading, watching or listening to content, typically in the privacy of their homes or other private spaces.

Like other forms of surveillance, the kind of DRM-based surveillance and data gathering described above can invade privacy in and of itself. However, because of the nature of the activities people are engaged in while being watched by DRM, DRM may also invade privacy in the sense of reducing the scope of our autonomy and intellectual freedom. In other words, knowledge that one's reading, writing, viewing and listening habits are being monitored may cause many people to avoid accessing or exploring certain forms of content.

PIPEDA Challenges

DRM unquestionably involves the collection, use and disclosure of personal information. Indeed, in the recent *SOCAN v. CAIP*⁸ decision Justice LeBel lent support to the idea that the kind of information processed by DRM is sensitive personal information:⁹

[an individual's surfing and downloading activities] tend to reveal core biographical information about a person. Privacy interests of individuals will be directly implicated where owners of copyrighted works or their collective societies attempt to retrieve data from Internet Service Providers about an end users downloading of copyrighted works.

Obviously if privacy is implicated where copyright industries attempt to gather such data from ISPs, then privacy is also implicated where the same and even more detailed information is gathered directly from individuals through DRM. Further, potential privacy problems may be amplified by the lack of a judicial process in the direct collection and use of personal information through DRM. This kind of information, or at least its connection to an identifiable individual, has typically only been available to copyright owners through a judicial process under PIPEDA such as that in the *BMG Canada* case.

In some ways, DRM may actually create new forms of personal information, at least to the extent that the information it collects is not information we previously conceived as being collectable. For example, one new

form of information that might be 'created' by DRM is information about the fact that someone does *nothing* with a copyright work after they purchase it.

The privacy responsibilities and risks that might arise with DRM could be awesome. Consider, for example, that the Recording Industry Association of America has indicated interest in a biometric authentication component for DRM. This could require users to provide fingerprints in order to access or use content.¹⁰

It may be difficult to reconcile the operation of DRM with the requirements of PIPEDA. For example, as a potentially surreptitious and continuous surveillance system, DRM tends to maximize, not limit, the collection and use of personal information. Assuming that consent provisions would be included in licences managed by DRM, there is also some question as to whether such consents would be meaningful and adequate, as in other e-commerce contexts where standard form licences arise. The following statement appeared in a recent study of actual DRM-enabled content delivery systems, conducted by law professor, masters. student and law student:¹¹

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.

Although these and other challenges may arise under PIPEDA, there are two recent decisions under the Act that might support DRM-based surveillance. First, under a recent finding of the Privacy Commissioner dealing with a continuous telephone connection to a satellite television unit (Summary 276), DRM surveillance might be upheld for billing purposes and for the specific purpose of detecting and acting on unauthorized use of copyright works.

Second, if a DRM operator structured the collection and use of personal information on the surveillance camera model at issue in the *Eastmond v. CPR* case,¹² then DRM surveillance without consent could be upheld under s. 7 of the Act.¹³ In *Eastmond*, CPR used video cameras to record activities in its Toronto yard. These recordings were kept in a locked area and were never viewed unless an incident took place in the yard. If no incidents were reported, the recordings were destroyed within 96 hours. Although the finding may prove controversial in future cases, the court in

Eastmond held that because of the way CPR set up its system, “collection” only took place when an incident was reported and a video recording was viewed. If a DRM system was able to operate in similar fashion, then it might be upheld under the Act on this analysis.

Conclusion

This article has attempted to briefly introduce some of the conflict that has arisen between copyright and privacy, provide a basic overview of DRM technology and sketch some of its possible privacy implications, including a short discussion of PIPEDA. Although beyond the scope of this article, I have argued elsewhere that privacy can in fact be infused into DRM and that the interests of the copyright industries, ISPs, DRM engineers and the public all support striving toward that goal.¹⁴ It is hoped that this brief introduction will contribute to an increased awareness regarding DRM and privacy. This awareness is particularly important and timely because Canada is contemplating laws that would protect DRM.

** Alex Cameron was successful counsel for the Canadian Internet Policy and Public Interest Clinic <www.CIPPIC.ca> in the BMG Canada v. John Doe file-sharing case referenced in this article. Alex is currently pursuing his academic studies on leave from Fasken Martineau DuMoulin LLP where he practises in the areas of technology, intellectual property and privacy law. He can be reached at <acameron@uottawa.ca>.*

¹ [2004] F.C.J. No. 525 (QL) [hereinafter *BMG Canada*].

² *Recording Industry Ass'n of America v. Verizon Internet Services Inc.*, 2003 U.S. App. LEXIS 25735; *certiorari* denied, 2004 U.S. LEXIS 6700 (U.S. October 12, 2004).

³ *BMG Canada*, at paras. 20 and 42.

⁴ Microsoft Corporation appears to have deleted this definition from its current Web site and replaced it with a definition found at the following link, “Definition of DRM”, on-line: Microsoft <http://www.microsoft.com/windows/windowsxp/experiences/glossary_a-g.asp#drm>.

⁵ For a more detailed study of DRM technology, see Ian Kerr, Alana Maurushat, & Christian S. Tacit, “Technical Protection Measures: Part I — Trends in Technical Protection Measures and Circumvention Technologies” (2003), on-line: Heritage Canada <http://www.pch.gc.ca/progs/ac-ca/progs/pda-cpb/pubs/protection/tdm_e.cfm>.

⁶ John Perry Barlow, “Life, Liberty and the Pursuit of Copyright?” (September 17, 1998).

⁷ Information and Privacy Commissioner/Ontario, “Privacy and Digital Rights Management (DRM): An Oxymoron?” (October 2002) <<http://www.ipc.on.ca/docs/drm.pdf>>. See also <<http://www.epic.org/privacy/drm/>>.

⁸ *Society of Composers, Authors and Music Publishers of Canada v. Canadian Association of Internet Providers*, [2004] S.C.J. No. 44 (QL) [hereinafter *SOCAN*].

⁹ *SOCAN*, at para. 155.

¹⁰ See, e.g., Andrew Orłowski, “RIAA wants your fingerprints”, *The Register* (June 4, 2004), on-line: The Register <http://www.theregister.co.uk/2004/06/04/biometric_drm/>;

Dinesh C. Sharma, "Gateway adds fingerprint sensor to note book" *News.com* (March 24, 2004), on-line: News.com <http://news.com.com/2100-1044_3-5178842.html>.

¹¹ Deirdre K. Mulligan, John Han & Aaron J. Burstein, "How DRMbased content delivery systems disrupt expectations of 'personal use'" in *Proceedings of the 2003 ACM workshop on Digital rights management* (New York: ACM Press, 2003), 77.

¹² *Eastmond v. Canadian Pacific Railway*, [2004] F.C.J. No. 1043 (QL).

¹³ For a discussion of this case, see Norm Trerise, Alexis Kerr and Alex Cameron, "*Eastmond v. Canadian Pacific Railway*: Federal Court Approves Railway's use of Video Surveillance as a Security Measure and Investigative Tool" (2004) 11 C.P.L.R. 121.

¹⁴ Alex Cameron, "Infusing Privacy Norms in DRM: Incentives and perspectives from law" in *Proceedings of the 2004 IFIP World Computer Congress* [forthcoming in 2004].