3. LEARNING FROM DATA PROTECTION LAW AT THE NEXUS OF COPYRIGHT AND PRIVACY

ALEX CAMERON

I. INTRODUCTION

This chapter is a small part of a broader project[1] aimed at formulating principles and rules to account for intellectual privacy—individuals' freedom to access and enjoy creative works anonymously or in private—within the legal concept of copyright. The broader project argues that such principles and rules have heretofore been wanting in copyright, and that they are an essential component of copyright as a consistent and unified whole.

This chapter contributes to the goals of the broader project in two specific ways. First, the section entitled "Intellectual Privacy under Strain" describes some of the challenges posed by the use of digital technologies in association with copyright works. Second, in the section entitled "Lessons from Data Protection Law," this chapter considers whether data protection laws may stimulate important questions and provide guidance in governing digital copyright practices that involve monitoring individuals' access to and use of creative works. This chapter concludes with a look ahead to further work to be done in the area.

1. The broader project is the subject of the author's doctoral dissertation, in progress at the time of writing.

II. INTELLECTUAL PRIVACY UNDER STRAIN

A. The Analogue World

For nearly three centuries following the enactment of the world's first modern copyright statute,[2] neither copyright law nor copyright holders interfered with individuals' privacy. Neither *Rights of Man*[3] nor *The Clockmaker*[4] were delivered to readers on condition that they provide detailed personal information to the author, publisher, or bookseller; nor were readers monitored in their enjoyment of the works.[5]

Until relatively recently, individuals accessed and enjoyed creative works—including books, magazines, newspapers, scholarly periodicals, films, and music—almost exclusively in tangible form by purchasing a copy of the work at a retail store, visiting a library, or attending a public performance. These forms of "analogue" access to creative works usually afforded individuals a high degree of intellectual privacy. Once an individual had purchased or otherwise accessed a copy of a work, his or her relationship with the copyright holder or the distributor of the work ended; it was normally up to the individual to determine how, when, and under what conditions he or she enjoyed the work, subject of course to the terms of copyright law.

Even if copyright holders or others had been interested in monitoring individuals' access to and use of creative works, they had no practical means to do so; nor did they have any practical means to control individuals' activities or to enforce an ongoing license arrangement with them to govern use of the works. In light of these realities of the pre-digital world, copyright law and copyright holders were traditionally concerned exclusively with the activities of competing publishers, not individuals; the former group directly threatened copyright holders' economic interests, whereas individual consumers did not.

---

2. Copyright Act 1710 8 Ann c 19 [hereinafter Statute of Anne]. The Statute of Anne is sometimes referenced as originating in 1709. For an explanation of the reason for this historical discrepancy, see L. R. Patterson and Stanley W. Lindberg, *The Nature of Copyright: A Law of Users' Rights* (Athens, Georgia: University of Georgia Press, 1991), Chapter 2, note 22.

3. Thomas Paine, *Rights of Man* (London: J.S. Jordan, 1791).

4. Thomas Chandler Haliburton, *The Clockmaker, or, The Sayings and Doings of Samuel Slick, of Slickville* (Halifax: J. Howe, 1836).

5. In the case of the *Rights of Man*, the British government might very well have wished to have records of who purchased and who read the book. Paine was tried and convicted in absentia as author of a "seditious and libellous" work. See generally Thomas Paine, *The Political Writings of Thomas Paine: To which is Prefixed a Brief Sketch of the Author's Life, Volume I* (Charlestown: G. Davidson, 1824), xi. It should also be noted that both *Rights of Man* and *The Clockmaker* have been digitized and are available for download on the Internet—this point is revisited in section D(3) of this chapter.

Contrasted against this historical backdrop, late in the twentieth century and continuing into the twenty-first century—concurrent with the rise and spread of digital networks and the increasing digitization of copyrighted works—the centuries-old relationship between copyright holders and individuals became strained. More particularly, the relationship between copyright law, copyright holders, and individuals' intellectual privacy came into tension.[6] This tension is not altogether new; librarians, for example, traditionally respected the value of intellectual privacy and enforced strict protections against the disclosure of patrons' borrowing records. However, libraries are no longer the only source, or even a primary source, of information about individuals' access to creative works and other information products; far from it. We cannot rely on only our libraries to protect our intellectual privacy; we must decide more broadly whether and how to preserve the value of intellectual privacy in the digital age.[7]

B. The Digital Age

With the advent of the digital age, individuals were eager to explore new ways of using digital technologies, especially computers, to access and enjoy creative works. Many copyright holders were eager to meet the demand for digital works, to reap the benefits of digital distribution, and to pursue new business models for exploiting works. At the same time, however, they were wary of the fact that digital technologies offered "the man on the Clapham omnibus"[8] a virtually effortless means, for example, to make and manipulate perfect copies of digital works and share them with millions of other individuals, without the knowledge or permission of the copyright holder and often in violation of copyright law. The most widely-known example of this activity is peer-to-peer file sharing of music using the products and services offered by, among others, the original Napster service.[9]

---

6. The "digital age" or the "information age" could be considered to have started with the invention of the first digital computers during World War II. It was not, however, until the 1990s and into the twenty-first century that the "digital age" became truly relevant and revolutionary for copyright, particularly with the explosive growth in mainstream popularity of personal computers and the Internet which occurred during this period.

7. Lessig puts a closely related question as follows: "In a world where this monitoring could not effectively occur, there was, of course, no such right against it. But now that monitoring can occur, we must ask whether the latent right to read anonymously, given to us before by imperfections in technologies, should be a legally protected right." Lawrence Lessig, *Code Version 2.0* (New York: Basic Books, 2006), 191.

8. "The man on the Clapham omnibus" refers to an ordinary, average person. The term is a legal fiction of the "average" and "reasonable" citizen, first adopted in legal circles in *McQuire v Western Morning News* [1903] 2 KB 100 (CA) 109.

9. For a description of how the original Napster service operated, see *A&M Records, Inc. v Napster, Inc.*, 239 F.3d 1004 (9th Cir. 2001).

Many copyright holders thus legitimately perceived and continue to perceive the digital realm as both an opportunity and a threat; it is in the responses to the characteristics of the digital realm that the relationship between copyright and privacy has been most profoundly implicated. For example, in order to pursue the opportunities and to mitigate the threats of digital networks, many copyright holders and others who distribute copyrighted works turned to technological means to attempt to control individuals' access to and enjoyment of copyright works, and to prevent copyright infringement. Such technological means include digital rights management (DRM) and related technology systems.

In general terms, DRM technologies are embedded in software, hardware, or both, and travel with digital works in order to regulate access to and use of the works. DRM is a kind of "digital lock." DRM technologies used to control a song, for example, might enforce a "listen but don't share" permission, restricting the ability of individuals to copy the song to more than one computer or portable device, such as a mobile phone or iPod.[10] DRM technologies continue to evolve and are used by contemporary copyright holders and others across many different forms of works.[11]

It is perhaps not surprising that DRM technologies have sparked controversy on a number of fronts.[12] DRM technologies are relevant for the purposes of this chapter because they are emblematic of the strain in the relationship between copyright and privacy experienced to date in the digital age. In ostensibly exploiting copyrighted works and preventing copyright infringement, many DRM technologies and the licensing practices that they enable depend in part on identifying and tracking copyrighted works, as well as the individuals who access and use them.[13]

---

10. Conditions that could potentially be enforced through such technologies are limited virtually by the imagination, including, for example, "Do not copy more than 5 times," "Do not modify," "Do not print," and "Do not save as a different file format."

11. For a review of privacy-implicating DRM in use in the Canadian market, see Canadian Internet Policy and Public Interest Clinic (CIPPIC), "Digital Rights Management and Consumer Privacy: An Assessment of DRM Applications under Canadian Privacy Law" (2007) <http://www.cippic.ca/uploads/CIPPIC_Report_DRM_and_Privacy.pdf> [CIPPIC Study]. The author of this chapter contributed to the CIPPIC study.

12. Among other issues, one of the important issues raised by DRM relates to competition law and policy. See, e.g., Alex Cameron and Robert Tomkowicz, "Competition Policy and Canada's New Breed of 'Copyright' Law" (2007) 52 McGill LJ 291.

13. See, e.g., Ian R. Kerr, Alana Maurushat, and Christian S. Tacit, "Technological Protection Measures: Part I—Trends in Technical Protection Measures and Circumvention Technologies" (2003) at s 5.2.2, http://www.pch.gc.ca/progs/ac-ca/progs/pda-cpb/pubs/protection/5_e.cfm ("In order to carry out their proper function, DRMs collect, process, and in some cases, store personal information. DRMs may also closely monitor and track the use of digital content. In effect, DRMs can identify consumers and create profiles that identify individual consumer consumption patterns. While the proper use of such personal information can be positive for those consumers who wish to receive customized

Many forms of DRM use a monitoring mechanism as a component of controlling access to and use of creative works.[14] In many cases, DRM operation is fundamentally premised on a diminishment of individuals' intellectual privacy since, through the collection of information about individuals' access to and use of copyrighted works, DRM reduces or eliminates individuals' freedom to access and enjoy copyrighted works anonymously or in private. Although there are many examples of this diminishment, it is worth briefly noting one for demonstrative purposes.

eReader offers a catalog of over 17,000 electronic books for sale on its Web site.[15] An individual downloads the purchased book, installs the eReader software, enters his or her password—which is in fact his or her credit card number[16]—to unlock the book, and is then able to read it.[17] In its privacy policy, eReader candidly states that it profiles its customers:

> We store information that we collect through your stated preferences, cookies, log files, clear gifs, and/or third party sources to create a "profile" of your preferences. We tie your personally identifiable information, and your activity history, to information in the profile, in order to provide tailored promotions and marketing offers and to improve the content of the site for you.[18]

Although it is not clear whether this profiling is directly linked to the operation of the software controlling access to the e-books, it is clear that eReader collects profiling information as part of its interactions with its customers, and that it transmits data during operation of the eReader software.[19] Data collected could include a list of book searches or book titles purchased. Additionally, an appreciation for the full scope of information that the software could be collecting and

---

services, the tremendous potential for acquisition of personal information also gives rise to serious privacy concerns." (footnotes and citations omitted)). See generally L.A. Bygrave, "Digital Rights Management and Privacy—Legal Aspects in the European Union," in *Digital Rights Management-Technological, Economic, Legal and Political Aspects,* Eberhard Becker et al., eds. 418–446 (Berlin: Springer-Verlag, 2003). See also Deirdre K. Mulligan, John Han and Aaron J. Burstein, "How DRM-Based 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.

14. See, e.g., Kerr and others "Technological Protection Measures: Part I," 5.2.2 (n. 13).

15. eReader http://www.ereader.com/.

16. eReader, "Frequently Asked Questions" http://www.ereader.com/help/faq. The use of the credit card number as a password was criticized in the CIPPIC Study. See CIPPIC Study 35 (n. 11).

17. eReader, "An eBook Primer" http://www.ereader.com/help/intro.

18. eReader, "Privacy Policy" http://www.ereader.com/ereader/privacy.htm. CIPPIC Study 47 (n. 11).

19. CIPPIC Study 61 (n. 11).

reporting back to eReader can be gained by considering that the software "eReader Pro for Windows" is capable of the following functions:

> . . . while reading your book you can select any word and easily look it up using your included Merriam-Webster's Pocket Dictionary . . .
>
> . . .
>
> Create detailed notes about your reading and share them with others.
>
> . . .
>
> Highlight key words to remember them later.
>
> . . .
>
> Add and organize book marks with the click of a mouse.[20]

Subject to considerations about whether meaningful consent was obtained from affected individuals, privacy interests would naturally be implicated if, in its customer profiling, eReader is collecting, using, or disclosing the forms of detailed information identified in this passage.

C. The Broad Questions

eReader provides one example of the kinds of conflict that can arise between copyright and privacy.[21] Although this specific example and others like it may be resolved or rectified, their resolution is not determinative of the overarching questions that they raise about the intersection between copyright and intellectual privacy. To use a traffic analogy, the resolution of specific cases of conflict between copyright and intellectual privacy can be likened to two cars crashing at an intersection: the cars may be towed away after the accident, but the intersection itself may be dangerous and in need of repair.

Through the use of many forms of DRM, individuals are increasingly unable to experience creative works anonymously or in private; knowingly and unknowingly, they routinely disclose their personal information and are technologically monitored when searching for, accessing, and enjoying copyrighted works. These conditions are the norm facing individuals wishing to access and enjoy many modern forms of digital works. Indeed, conflict between copyright and intellectual privacy has reached a point where some of the most fundamental questions about the appropriate limits of copyright holders' rights are virtually synonymous with questions about the appropriate limits of intellectual privacy in connection with the enjoyment of creative works. To date, the consequence of this conflict has been a diminishment of individuals' intellectual privacy. Should this conflict continue on its current path, we may be left with little or no room to travel our vibrant copyright kingdoms anonymously or in private.

---

20. eReader, "eReader Pro for Windows Software" http://www.ereader.com/ereader/software/product/15009_pro_win.htm.

21. For other examples, see CIPPIC study (n. 11).

It is possible that the increasing diminishment of intellectual privacy will be halted or reversed. Any number of changes in technology, markets, and regulation may influence the course of intellectual privacy in one direction or another.[22] There are, for example, a number of recent indications that DRM has been dropped in connection with some music downloads[23] and audio books[24] (though it is not clear that enhanced intellectual privacy will result from these developments).[25] Further, from time to time, specific privacy-invasive practices of copyright holders are brought to light, found to be illegal, and redressed. Copyright holders are among the first to acknowledge that, where applicable, data protection laws of general application operate to restrict some activities that diminish individuals' intellectual privacy. The application of such laws is discussed in the next section of this chapter. Commentary and debate over these questions continues.

Yet, predicting the future state of copyright, technology, the market, or intellectual privacy is not object of this chapter. We may end up in a world where we "tap into the beam"[26] and have digital access to every book ever published—then again, we may not. Irrespective of what the future may hold, the presently observable diminishment of intellectual privacy has, per se, brought to the fore some critical, previously unexplored questions about the relationship between copyright and intellectual privacy. The time is ripe to consider questions that have floated, ignored and obscured, through copyright and privacy discourses for centuries. Central among these questions is the domain of the broader project—the value and role of intellectual privacy *within* the legal concept of copyright—of which this chapter is a part.

The next section of this chapter reviews how data protection law may contribute to, or otherwise inform, a broader analysis of the potential role of intellectual privacy within copyright.

III. LESSONS FROM DATA PROTECTION LAW

A. Background

Privacy regulators and policy makers are aware of the mounting tension between copyright and intellectual privacy, and have focused increased attention

22. Daniel Gervais introduced this "technopolicy triangle." See Daniel J. Gervais, "The Price of Social Norms: Towards a Licensing Regime for File-Sharing" *Journal of Intellectual Property Law* 12, no. 1 (2005): 39–74.

23 See Yinka Adegoke, "Sony BMG to Drop Copy Protection for Downloads" *Reuters* (January 7, 2008).

24 See Richard Wray, "Penguin Audiobooks to be Free of Copyright Protection" *The Guardian* (March 4, 2008).

25 See Bill Rosenblatt, "What Does "DRM-Free" Mean?" *DRM Watch* (June 7, 2007).

26 David Gelernter, "Tapping into the Beam," in *The Next Fifty Years: Science in the First Half of the Twenty-First Century*, John Brockman ed. (New York: Vintage Books, 2002) (offering a prediction of the state of computer technology in or about the year 2050).

on the matter. The European Union Data Protection Working Party, for example, recently expressed concern about "the fact that the legitimate use of technologies to protect works could be detrimental to the protection of personal data of individuals."[27] Canada's privacy community has voiced similar concern regarding DRM, particularly in the context of possible legislation that would protect the use of DRM.[28] A number of Canada's privacy commissioners have echoed this concern.[29]

There is also a developing contemporary literature and body of law at the intersection of copyright and intellectual privacy. Leading academics, public interest groups, business leaders, policy makers, regulators, courts, and others are increasingly engaged in a global dialogue on the topic. Courts, for example, are increasingly faced with, and must decide, cases where copyright interests are seen as pitted against privacy interests.[30] In addition, concerned about the

27. Article 29 Data Protection Working Party, "Working Document on Data Protection Issues Related to Intellectual Property Rights" WP104 (18 January 2005), http://ec.europa.eu/justice_home/fsj/privacy/docs/wpdocs/2005/wp104_en.pdf (accessed March 7 2008).

28. See Canada's Privacy Community, "Letter from Canada's Privacy Community to Ministers Bernier and Oda" (May 17, 2006) http://www.intellectualprivacy.ca/documents/open_letter.pdf; Canada's Privacy Community, "Background Paper: Critical Privacy Issues In Canadian Copyright Reform" (May 17, 2006) http://www.intellectualprivacy.ca/documents/background_paper.pdf.

29. See Letter from Jennifer Stoddart, Privacy Commissioner of Canada, to Ministers Prentice and Verner (January 18, 2008), http://www.privcom.gc.ca/parl/2008/let_080118_e.asp; Letter from Jennifer Stoddart, Privacy Commissioner of Canada, to Ministers Oda and Bernier (May 17, 2006), http://www.privcom.gc.ca/media/let/let_ca_060517_e.asp; Letter from David Loukidelis, Information and Privacy Commissioner of British Columbia, to Ministers Oda and Bernier (May 17, 2006), http://www.oipcbc.org/publications/Comm_Public_Comments/F06-28751.pdf; Open Letter from Ann Cavoukian, Information and Privacy Commissioner of Ontario, to Ministers Oda and Bernier (May 12, 2006), http://www.ipc.on.ca/docs/drmletter.pdf; Letter from Frank Work, Information and Privacy Commissioner of Alberta, to Ministers Oda and Bernier (May 26, 2006), http://www.oipc.ab.ca/ims/client/upload/Copyright_ltr_May_26_06.pdf. The Office of the Privacy Commissioner of Canada has also since issued a Fact Sheet regarding DRM that includes the following statement: "The use of TPMs, however, can seriously affect the privacy rights of individuals, and by invading their privacy and reporting on their behaviour, impact other civil liberties such as freedom of association and freedom of expression. While rights holders have a perfectly legitimate view of the matter, it is also reasonable to expect them to enforce their rights only in a way which respects individual privacy rights." See Office of the Privacy Commissioner of Canada, "Fact Sheet: Digital Rights Management and Technical Protection Measures" (November 2006), http://www.privcom.gc.ca/fs-fi/02_05_d_32_e.asp.

30. See *BMG Canada Inc. v Doe* [2005] 252 DLR (4th) 342; 2005 FCA 193 (CanLII) ("Although privacy concerns must also be considered, it seems to me that they must yield to public concerns for the protection of intellectual property rights in situations where infringement threatens to erode those rights." paragraph 41); *Society of Composers, Authors*

potential consequences of yielding individuals' intellectual privacy where it conflicts with copyright holders' interests, academic commentators have conducted widespread reconnaissance for support of intellectual privacy; these inquiries have spanned, among others, freedom of expression,[31] data protection,[32] human rights,[33] and ethics.[34] It is only a matter of time before a complaint is brought under data protection law.

B. Surveillance and Related Jurisprudence under Canada's Data Protection Law

This section briefly reviews surveillance and related monitoring cases under a well-known data protection law based on fair information practices and approved by the European Community[35] as providing adequate protection: Canada's federal data protection law, the Personal Information Protection and Electronic Documents Act.[36]

Except in situations where provincial laws apply, PIPEDA regulates the collection, use, and disclosure of personal information in the private sector in Canada. The Act contains a number of obligations to which organizations must adhere in

and Music Publishers of Canada v Canadian Assn. of Internet Providers, [2004] 240 DLR (4th) 193; 2004 SCC 45 (CanLII) [*SOCAN v CAIP*].

31. See Julie Cohen, "A Right to Read Anonymously: A Closer Look at 'Copyright Management' in Cyberspace," *Conn.* L. Rev 28 (1996): 981 (evaluating the import of diminished intellectual privacy for traditional notions of freedom of expression and freedom of thought).

32. See Graham Greenleaf, "IP, Phone Home: Privacy as Part of Copyright's Digital Commons in Hong Kong and Australian Law" in *Hochelaga Lectures 2002: The Innovation Commons*, ed. Lawrence Lessig (Hong Kong: Sweet & Maxwell Asia, 2003) (asserting that amendments to copyright law and data protection law may be needed to protect intellectual privacy); Ian Kerr, "If Left to Their Own Devices . . . How DRM and Anti-circumvention Laws Can Be Used to Hack Privacy" in *In the Public Interest: The Future of Canadian Copyright Law*, ed. Michael Geist (Toronto: Irwin Law, 2005) 167–210.

33. See P. Bernt Hugenholtz. "Caching and Copyright," (2000) 22 European Intellectual Property Review 482, 485–486.

34. See Ian Kerr, "DRM & the Automation of Virtue" (Keynote presentation to Identity and Identification in a Networked World, September 2006) http://idtrail.org/content/view/542/42/.

35. In December 2001, the Commission of the European Communities issued Decision 2002/2/EC pursuant to Article 25(6) of 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, OJ L 281, 23.11.1995, p. 31. Decision 2002/2/EC states that Canada is considered as providing an adequate level of protection of personal data transferred from the European Community to recipients subject to PIPEDA.

36. Personal Information Protection and Electronic Documents Act SC 2000 c. 5 (Canada) [PIPEDA].

their handling of personal information, organized roughly around the following ten principles listed in the Act:

(1) Accountability
(2) Identifying Purposes
(3) Consent
(4) Limiting Collection
(5) Limiting Use, Disclosure, and Retention
(6) Accuracy
(7) Safeguards
(8) Openness
(9) Individual Access
(10) Challenging Compliance

Subsection 5(3) of PIPEDA contains an over-arching requirement under the Act that cannot be waived by consent or any other exception—it requires organizations to collect, use, and disclose personal information "only for purposes that a reasonable person would consider are appropriate in the circumstances."[37] This section is central in surveillance cases under PIPEDA, which are among the most frequently occurring and contentious cases.

Section 7 can also arise in surveillance cases. This section contains a number of exceptions to the general requirement to obtain consent for the collection, use, and disclosure of personal information. For example, paragraph 7(1)(b) permits the collection of information without consent if

> . . . it is reasonable to expect that the collection with the knowledge or consent of the individual would compromise the availability or the accuracy of the information and the collection is reasonable for purposes related to investigating a breach of an agreement or a contravention of the laws of Canada or a province.[38]

Organizations often rely on this exception when using surveillance to investigate or deter crime or to investigate employee misconduct.

The leading surveillance case under PIPEDA is *Eastmond v. Canadian Pacific Railway*.[39] In this case, employees filed a complaint after their employer, Canadian Pacific Railway (CPR), installed video cameras in a rail yard where the employees worked. The cameras captured fixed areas of the yard and had no

37. PIPEDA, s. 5(3) (n. 36).
38. PIPEDA, s. 7(1)(b) (n. 36).
39. Office of the Privacy Commissioner of Canada, "PIPEDA Case Summary #114: Employee Objects to Company's Use of Digital Video Surveillance Cameras" (November 6, 2003) http://www.privcom.gc.ca/cf-dc/2003/cf-dc_030123_e.asp; *Eastmond v Canadian Pacific Railway* [2004] 16 Admin LR (4th) 275 (FC). The author was a member of the legal team acting for Canadian Pacific Railway in this case.

ability to pan or zoom. CPR retained the recordings for a short time in a locked cabinet. The tapes were overwritten and never viewed if no incidents were reported. The recordings were not monitored or reviewed by CPR for any other purpose.

CPR claimed that it had a legitimate need to install the cameras for the following purposes: deterring incidents of theft, vandalism, and trespassing, improving employee security, and aiding in the investigation of incidents.

The Commissioner applied a four-part test under subsection of 5(3) of PIPEDA in determining whether a reasonable person would find CPR's stated purposes to be appropriate. The Federal Court agreed to be guided by the test in this case and made the following findings, summarized after each item of the test:

(i) *Is camera surveillance and recording necessary to meet a specific need?*
CPR had established a legitimate need to install the cameras based on a history of incidents at the yard, and acceptance of the cameras' deterrent effects.

(ii) *Is camera surveillance and recording likely to be effective in meeting that need?*
The lack of incidents since the cameras had been installed showed that the cameras were effective.

(iii) *Is the loss of privacy proportional to the benefit gained?*
Security benefits were tangible and privacy loss was minimal (1) the recording took place where individuals had a reduced expectation of privacy and (2) CPR had taken a number of steps to ensure that the invasion of privacy was minimal.

(iv) *Is there a less privacy-invasive way of achieving the same end?*
CPR had considered and rejected other more costly alternatives, including fences and security guards.

The court upheld CPR's installation of the cameras under PIPEDA. The *Eastmond* four-part test has also been applied in subsequent cases; other leading cases include a case where the Commissioner held that a credit card company can monitor individuals' purchasing history in order to detect fraud and for other purposes.[40] A similar finding was issued in the copyright context where the Commissioner upheld the use of a continuous telephone connection to a satellite television unit for billing purposes and for the specific purpose of detecting and acting on unauthorized use of copyrighted works.[41] In doing so, however,

40. Office of the Privacy Commissioner of Canada, "PIPEDA Case Summary #296: Language of Consent and Monitoring Activity Challenged" (April 20, 2005) http://www.privcom.gc.ca/cf-dc/2005/296_050314_02_e.asp.

41. Office of the Privacy Commissioner of Canada, "PIPEDA Case Summary #276: The Privacy Implications of Pay Per View and Piracy Prevention Measures" (September 27, 2004) http://www.privcom.gc.ca/cf-dc/2004/cf-dc_040902_01_e.asp.

the Commissioner was careful to note that the system was not collecting information about individuals' viewing habits.

Finally, in a landmark 2007 case involving violations of PIPEDA by TJX, operator of Winners and HomeSense stores,[42] the Commissioner agreed to permit TJX to collect drivers' licenses and other information for fraud prevention in the context of receipt-less merchandise returns. In past cases, the Commissioner had stated that collecting this information was inappropriate and unnecessary in this context.[43] In this case, however, the Commissioner deviated from past findings and accepted that TJX could collect the information on condition that it immediately convert the information to unique numbers using a cryptographic hashing function. This technique would convert the license numbers into a unique new number referred to as a "hash value," therein rendering the drivers' license numbers unreadable to TJX employees. The drivers' license information would be retained only temporarily for this purpose.

C. Preliminary Questions

Before turning to the elements of the four-part test under PIPEDA, it is important to briefly note that the question of whether a reasonable person would find DRM monitoring appropriate is only one of the questions that would need to be assessed in determining whether such practices are in compliance with data protection law.

Personal Information First, under PIPEDA or another data protection law, DRM monitoring would have to involve a collection, use or disclosure of "personal information"[44] or "personal data"[45] in order for the law to apply. The answer to this question depends on precisely what information a DRM system collects and whether it can be linked to an identifiable individual, even if the individual is not actually identified by the information. The answer is highly contextual—for example, a name may be personal information if it is linked to other records; however, if it is not linked to other records, then it may not be

42. Office of the Privacy Commissioner of Canada, "Report of an Investigation into the Security, Collection and Retention of Personal Information—TJX Companies Inc./ Winners Merchant International L.P." (September 25, 2007) http://www.privcom.gc.ca/cf-dc/2007/tjx_rep_070925_e.asp.

43. Office of the Privacy Commissioner of Canada, "PIPEDA Case Summary #361: Retailer Requires Photo Identification to Exchange an Item" (February 23, 2007) http://www.privcom.gc.ca/cf-dc/2006/361_20061114_e.asp. See also, Office of the Privacy Commissioner of Canada, "Settled Case Summary #16: Personal Information on Receipts Removed, Return Information Limited" (February 13, 2006) http://www.privcom.gc.ca/ser/2005/s16_051121_e.asp.

44. PIPEDA, ss. 2(1) & 4(1) (n. 36).

45. See U.K., Data Protection Act 1998 c. 29 s. 1(1) (definition of "personal data").

personal information.[46] The Federal Court of Canada has adopted the following definition of "personal information" developed by the Commissioner:

> Information will be about an identifiable individual where there is a serious possibility that an individual could be identified through the use of that information, alone or in combination with other available information.[47]

There are indications that DRM monitoring would often involve personal information. For example, in *SOCAN v. CAIP*, Justice LeBel of the Supreme Court of Canada lent support to the idea that the kind of information processed by DRM is sensitive personal information:

> . . . [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.[48]

This statement, that privacy is implicated where copyright holders attempt to gather data from ISPs, suggests that privacy is implicated where the same or even more detailed information is gathered directly from individuals through DRM monitoring. The lack of judicial process in the collection of information through DRM may aggravate potential privacy violations: in keeping with good public policy,[49] this kind of information has typically only been available to copyright owners through a judicial process.[50]

To make use of another example, there is a series of findings under PIPEDA holding that Internet protocol (IP) addresses are personal information.[51]

---

46. Office of the Privacy Commissioner of Canada, "PIPEDA Case Summary #205: What Is in a Name?" (November 6, 2003) http://www.privcom.gc.ca/cf-dc/2003/cf-dc_030805_03_e.asp.

47. *Gordon v Canada (Health)*, 2008 FC 258 (CanLII) ¶34. This case arose under the Privacy Act, R.S.C. 1985, c. P-21 and the Access to Information Act, R.S., 1985, c. A–1.

48. *SOCAN*, 155 (n. 30).

49. *Irwin Toy Ltd. v Doe* [2000] O.J. No. 3318 (S.C.J.) ("In keeping with the protocol or etiquette developed in the usage of the internet, some degree of privacy or confidentiality with respect to the identity of the Internet protocol address of the originator of a message has significant safety value and is in keeping with what should be perceived as being good public policy.").

50. See *BMG*, 37 (n. 30).

51. Office of the Privacy Commissioner of Canada, "PIPEDA Case Summary #25: A Broadcaster Accused of Collecting Personal Information via Web Site" (November 6, 2003) http://www.privcom.gc.ca/cf-dc/2001/cf-dc_011120_e.asp (accessed March 7, 2008); Office of the Privacy Commissioner of Canada, "PIPEDA Case Summary #315: Web-Centred Company's Safeguards and Handling of Access Request and Privacy Complaint Questioned" (August 31, 2005) http://www.privcom.gc.ca/cf-dc/2005/315_20050809_03_e.asp; Office of the Privacy Commissioner of Canada, "PIPEDA Case Summary #319:

The European Union Data Protection Working Party has also concluded that IP addresses are personal data:

> The Working Party wishes to emphasize that IP addresses attributed to Internet users are personal data and are protected by EU Directives 95/46 and 97/66. . .
>
> In the case of IP addresses the ISP is always able to make a link between the user identity and the IP addresses and so may be other parties, for instance by making use of available registers of allocated IP addresses or by using other existing technical means.[52]

Since DRM will almost always involve the collection of IP addresses as part of its operation, along with other information that specifically identifies individuals (e.g., name, credit card information), DRM will in many cases almost certainly be subject to the application of data protection laws.

Consent Second, a host of questions arise around the issue of consent, a cornerstone of data protection laws. Subject to some exceptions, PIPEDA requires organizations to obtain consent from individuals for the collection, use, and disclosure of their personal information.[53]

It may be difficult to reconcile the operation of DRM with the requirement to obtain consent under data protection law. Consent provisions are typically included in privacy policies or in licenses managed by DRM. There is some question as to whether such consents are meaningful and adequate, as in other e-commerce contexts where standard-form licenses arise. The following statement appeared in a recent study of actual DRM-enabled content delivery systems:

> 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.[54]

Others have conducted exceptional analyses on the issue of consent and concluded that there are good reasons to believe that standard-form consents

---

ISP's Anti-Spam Measures Questioned" (February 13, 2006) http://www.privcom.gc.ca/cf-dc/2005/319_20051103_e.asp.

52. Article 29 Data Protection Working Group, "Opinion 2/2002 on the Use of Unique Identifiers in Telecommunication Terminal Equipments: The Example of IPV6" (May 30, 2002), http://ec.europa.eu/justice_home/fsj/privacy/docs/wpdocs/2002/wp58_en.pdf: 3.

53. PIPEDA, Principle 4.3 (n. 36).

54. Mulligan et al., "How DRM-Based Content Delivery Systems Disrupt Expectations of 'Personal Use,'" 84 (n. 13).

may be inadequate in connection with the operation of DRM, both as a broader public policy matter and as a matter of compliance with data protection law.[55] Kerr put the issue as follows:

> Like copyright, privacy law's compromise between the needs of organizations and the right of privacy of individuals (with respect to their personal information) will also be put in serious jeopardy if, irrespective of privacy rules, content owners are able to impose their terms and conditions through standard form contracts with complete impunity.[56]

Irrespective of the critical issue of consent, however, is the over-arching question of whether, despite a standard-form consent, an organization's use of DRM is an appropriate purpose under subsection 5(3) of PIPEDA.

D. Would the Man on the Clapham Omnibus Find DRM Monitoring Appropriate?

Is Monitoring Necessary to Meet a Specific Need? The question of need is an empirical matter weighed by the evidence submitted in support of or against a measure that diminishes privacy. In the *Eastmond* case, for example, CPR provided evidence of a history of incidents at its rail yards and argued that the surveillance was necessary to respond to those incidents.

In the case of DRM, there is conflicting broad-based evidence as to whether there is a need for monitoring access to and use of copyrighted works in order to prevent, deter, or investigate copyright infringement. Proponents of DRM assert that it is needed in order to protect copyrighted works against infringement in the digital realm, often pointing to economic studies about the losses of revenues that some copyright holders suffer as a result of infringement.[57] Opponents of DRM point to other studies which indicate that copyright infringement in the digital age has not had a net-negative economic impact on certain copyright holders.[58] Thus, on a macro level, there may be some question as to whether there is a specific need for DRM at all. Further, given that many copyright holders do not utilize DRM, and given that some copyright holders that have

55. See Kerr, "If Left to Their own Devices," (n. 32).

56. Kerr, "If Left to Their Own Devices," 192 (n. 32).

57. See Stan J. Liebowitz, "Economists Examine File-Sharing and Music Sales"in *Industrial Organization and the Digital Economy*, eds. G. Illing and M. Peitz (Cambridge: MIT Press, 2006) 145–174.

58. See Birgitte Andersen and Marion Frenz, "The Impact of Music Downloads and P2P File-Sharing on the Purchase of Music: A Study for Industry Canada" (October 30, 2007) http://strategis.ic.gc.ca/epic/site/ippd-dppi.nsf/en/h_ip01456e.html (accessed March 7, 2008); Felix Oberholzer-Gee and Koleman Strumpf, "The Effect of File Sharing on Record Sales An Empirical Analysis," *Journal of Political Economy*, 115 (2007): 1–42.

utilized DRM in the past have backtracked and dropped DRM,[59] the question of need is certainly an unsettled one.

On a micro level, however, a specific copyright holder may be able to show that it is in a unique situation that differs from industry-wide reports. For example, assume for the sake of argument that non-CPR rail yards in Canada typically do not have any security problems and in fact are 100% incident-free. All else being equal, one would assume that the result in *Eastmond* would nevertheless have been the same if CPR had been able to show, as it did, that *it* had a specific need at its rail yard.

The first element of the *Eastmond* test is difficult to apply to DRM monitoring, and is highly fact-specific. Despite the fact that there is broad-based disagreement as to whether alleged copyright infringement in the digital age has on the whole had a negative impact on copyright holders' interests, some organizations will likely be able to demonstrate a specific need—a specific history of copyright infringements—that they will be able to claim under PIPEDA necessitates adopting a monitoring solution.

Is Monitoring Likely to be Effective in Meeting That Need? Just as there is disagreement about whether there is a broad-based need for DRM monitoring, there is disagreement about whether DRM is effective in protecting copyrighted works against infringement. Some suggest that DRM monitoring is not and cannot ever be effective.[60]

Some copyright holders appear to conditionally agree with this conclusion, claiming that DRM technology will be ineffective if it is not protected by additional legal protections—called anti-circumvention laws: "As no technological measure can permanently resist deliberate attacks, a TPM is only as good as its legal protection."[61] Ineffectiveness of DRM may also be one of the reasons why many copyright holders who have experimented with DRM have recently reduced or discontinued its use.

As in the case of establishing a specific need for monitoring, the question of effectiveness is also highly fact-dependent. Specific organizations may be able to demonstrate that as a result of their market, works, technology, or other factors, their DRM monitoring would be effective. They may also be able to demonstrate that infringements declined or ceased following implementation of a DRM system.

---

59. See (n. 23–25) and accompanying text.

60. See Peter Biddle, Paul England, Marcus Peinado, Bryan Willman, "The Darknet and the Future of Content Distribution" in *Digital Rights Management* (Heidelberg: Springer, 2003) 155–176; Cory Doctorow, "Microsoft Research DRM Talk" (June 17, 2004) http://craphound.com/msftdrm.txt.

61. International Federation of the Phonographic Industry, "The WIPO Treaties: Technological Measures" (March 2003) http://www.ifpi.org/content/library/wipo-treaties-technical-measures.pdf.

The court in *Eastmond* was persuaded by CPR's evidence that no incidents had been reported since it had implemented its video surveillance system.[62]

Is the Loss of Privacy Proportional to the Benefit Gained? Proportionality is likely the single most important and controversial element of the test in the case of DRM. This element raises important questions about the value of intellectual privacy and how we ought to measure its loss. Recall that in Eastmond, the court considered relevant the fact that the cameras were in parking lots and other locations where there was a lower reasonable expectation of privacy, and that CPR had otherwise minimized the privacy impact of the cameras (including by not viewing the recordings unless incidents were reported). Proportionality thus depends in part on the interests of stake on both sides of the equation—it is both the value of the benefit and the value of the loss of privacy that must be considered.

In the context of DRM, it is possible that public and policy discourse regarding copyright in the digital age has disproportionately focused on the single issue of peer-to-peer (p2p) file-sharing of popular music and movies.[63] As a possible consequence, questions surrounding the resolution of digital copyright matters in general, including questions regarding intellectual privacy, may be viewed by some as being relatively trivial.[64] Some might conclude that activities such as listening to "Top 40" music and watching Hollywood movies, for example, like the parking lots in *Eastmond*, do not attract a strong expectation of privacy. For some, these categories of creative works might not *prima facie* implicate deeply-held notions regarding the importance of intellectual privacy in the same way that political or religious writings might.

As copyright works are increasingly disseminated in digital form, however, the stakes undeniably increase in the way that copyright's relationship with intellectual privacy is addressed. There are already signs that these stakes are increasing. Consider, for example, that the two books referenced at the outset of this introduction—*Rights of Man* and *The Clockmaker,* originally published in the eighteenth and early nineteenth century, respectively—have since been digitized

62. *Eastmond*, 179 (n. 39).

63. See Laura Murray, "Copyright Talk: Patterns and Pitfalls in Canadian Policy Discourses" in *In the Public Interest: The Future of Canadian Copyright Law*, ed. Michael Geist (Toronto: Irwin Law, 2005) 15–60, 27–28 (". . . music file-sharing is commonly taken to be the predominant Internet activity and policy problem that sets the tone for or even trumps all others.").

64. Murray "Copyright Talk" 30 (n. 63) (". . . the emphasis on music file-sharing may also make copyright reform seem less than earth-shaking: Members of Parliament might well wonder how important a bunch of teenagers ripping off music can be in the grand scheme of pressing government issues. This trivialization is unfortunate given the serious repercussions of the numerous details of copyright legislation for a growing range of economic and educational sectors.").

and are available for download on the Internet.[65] Indeed, as of early 2007, at least tens of thousands of books from libraries around the world were being digitized each week. Reports indicate that Google, one of the leaders in book digitization, "intends to scan every book ever published, and to make the full texts searchable, in the same way that Web sites can be searched on the company's engine at google.com."[66] Libraries and archives around the world are engaged in similar projects, as are publishers and book distributors.[67]

Using digitization to increase access to the information contained in books is certainly laudable; however, it does not come without risk. If DRM or other means of diminishing intellectual privacy were used in association with access to and use of *Rights of Man*, *The Clockmaker*, or "every book ever published," then the traditional relationship between copyright and intellectual privacy would be entirely rewritten. It is in access to books, newspapers, magazines, journal articles, and other media that questions of intellectual exploration, access to information, and intellectual privacy intuitively seem most sacred. Thus, far from being a problem circumscribed by interests at stake in "Top 40" music and Hollywood movies, the question of intellectual privacy is all the more patently pressing in light of the potential for the increasing digitization of literary works. The digitization of books is offered as an example here because it provides an easy insight into reasons why questions at the nexus of copyright and intellectual privacy are important.

Further, consistent with Justice LeBel's view that information about enjoyment of copyrighted works tends to reveal core biographical information about individuals,[68] there are good reasons to reject distinctions between various forms of copyrighted works when it comes to the application of the *Eastmond* test. Differences between "Top 40" music and Hollywood movies on the one hand, and political or religious writings on the other hand, ought not to bear to any

65. Both of these works have been digitized by Project Gutenberg and by Google. They are available for download at the following URLs: *Rights of Man* Project Gutenberg edition http://www.gutenberg.org/dirs/etext03/twtp210.txt, Google Books edition http://books.google.com/books?id=FKlNmiM4GJwC&pg=PA1&dq=rights±of±man, and *The Clockmaker* Project Gutenberg edition http://www.gutenberg.org/dirs/etext04/clckm10.txt, Google Books edition http://books.google.com/books?id=804lAAAAMAAJ&pg=PA1&dq=the±clockmaker&as_brr=1.

66. Jeffrey Toobin, "Google's Moon Shot: The Quest for the Universal Library" *The New Yorker* (February 5, 2007) 30–35, 30.

67. See University of Michigan Library, "One Million Digitized Books" (February 2, 2008) http://www.lib.umich.edu/news/millionth.html, (in partnership with Google); Cristina Jimenez, "British Library Books Go Digital" *BBC News* (September 28, 2007) http://news.bbc.co.uk/2/hi/technology/7018210.stm. The example of eReader was discussed earlier in this chapter. See also Reuters, "Report: Random House to Sell Book Chapters" (February 11, 2008) http://www.news.com/2110-1026_3-6229985.html.

68. *SOCAN*, 155 (n. 30).

significant degree—if at all—on whether an individual has an expectation of privacy in his or her enjoyment of the work. Anyone who has grown up with rock-and-roll music, for example, can attest to the importance that such music had on their identity and cultural development. Foucault offers the following view of the significance of rock music:

> Not only is rock music (much more than jazz used to be) an integral part of the life of many people, but it is a cultural initiator: to like rock, to like a certain kind of rock rather than another, is also a way of life, a manner of reacting; it is a whole set of tastes and attitudes.[69]

Is the loss of privacy proportional to the benefit gained in the case DRM? This is a difficult question. It may be inappropriate under PIPEDA to engage in such a broad-based consideration of the loss of privacy and proportionality. Perhaps the "loss" and the "benefit" ought to be confined to the specific case at issue. As in other elements of the test, there is a tension between focusing narrowly on the case at hand and focusing more broadly on the public policy ramifications of finding one way or another.

The loss of privacy may also be mitigated by other factors. For example, if an organization were to adopt the *Eastmond* "locked cabinet" approach to collecting personal information in DRM, then that would likely weigh in favor of it being found appropriate. Adopting an encryption approach along the lines described in the TJX case might also minimize privacy loss, making it more likely that the loss would be proportional to the benefit gained by the monitoring.

Is There a Less Privacy-Invasive Way of Achieving the Same End? Like the proportionality analysis, the final element in the *Eastmond* test is critical. Although *Eastmond* held that organizations are entitled to reject less privacy-invasive alternatives if they are more costly, alternatives must be properly considered.

In the case of DRM, there do appear to be less privacy-invasive ways of achieving the same end; DRM need not be inherently privacy-invasive. A number of commentators have noted that DRM design need not involve constant monitoring or the collection of personal information.[70] Ensuring that individuals are authorized to access or use particular content, which is a central purpose of DRM, does not necessarily require monitoring and the collection of personal information.

---

69. Michel Foucault, Pierre Boulez, "Contemporary Music and the Public" John Rahn Perspectives of New Music 24 no. 1 (1985), 6–12.

70. For a discussion of these proposals, see Alex Cameron, "Infusing Privacy Norms in DRM—Incentives and Perspectives from Law" in *Information Security Management, Education and Privacy, IFIP 18th World Computer Congress, TC11 19th International Information Security Workshops, 22–27 August 2004, Toulouse, France,* eds. Yves Deswarte, Frederic Cuppens, Sushil Jajodia and Lingyu Wang (Berlin: Kluwer, 2004): 293–309; Kerr "If Left to Their Own Devices," 183–185 (n. 32).

These alternative solutions may render privacy-invasive DRM inappropriate in most cases under the *Eastmond* test.

IV. CONCLUSIONS

The use of digital technologies to create, enjoy, and disseminate copyrighted works has highlighted tensions that have long existed between copyright and intellectual privacy. As part of a broader project aimed at reconciling those tensions within the copyright system, this brief chapter has crystallized some of the challenges posed by the use of digital technologies in association with copyrighted works. It is hoped that this discussion contributes to a clearer understanding of the issues between copyright and intellectual privacy, as well as what is ultimately and more broadly at stake.

This chapter also considered the application of data protection law to DRM practices. This jurisprudence is important for many reasons. For example, data protection laws are influential in shaping the future course of privacy in general. Through the repeated application of principles developed in the cases, including the *Eastmond* case, PIPEDA helps to guide the genesis of new technologies and practices. In other words, the DRM monitoring systems that PIPEDA helps to shape are the very systems that this author's broader project must account for in reconciling tensions between copyright and intellectual privacy within copyright.

The analysis under data protection law is also suggestive of possible questions that copyright might ask itself in designing principles and rules for addressing intellectual privacy within copyright. As suggested in some of the analysis in this chapter, however, there may be something of a disconnect under the data protection law analysis between results in particular cases and results that more broadly address the proper balance between competing copyright and intellectual privacy interests.

In other words, the *Eastmond* test might produce results in particular cases that may be at odds with a broader or higher-level balancing between copyright and intellectual privacy. Further, if certain forms of "lowbrow" copyrighted works were understood to be the equivalent of the parking lots in *Eastmond*—"places" where an individual's expectation of privacy is low or nonexistent—then the *Eastmond* test would fail to adequately recognize the biographical nature of copyrighted works and the potentially invasive profiling and diminishment of intellectual privacy that can result from monitoring individuals' activities in that context. Austin puts this potential shortcoming of the *Eastmond* test more generally as follows:

> . . . this test will not adequately protect privacy unless it includes, as a first step, an inquiry into the nature and extent of the privacy interest at stake.

> Without this, the test . . . [misses] the important initial step of defining the right in question and the manner in which it is being violated. Because of this, the danger is that this test for reasonable purposes will become a test for limiting privacy rather than enhancing it. To counter this danger, what is needed is a return to the very difficult questions involved in defining privacy and its value. In other words, fair information practices must grapple with, rather than avoid, the same challenges facing other regimes of privacy protection such as constitutional law.[71]

When applied at the nexus between copyright and privacy, data protection laws such as PIPEDA thus stimulate a number of questions and areas for future work. This work is needed especially if principles and rules to account for intellectual privacy within the legal concept of copyright are to bear any resemblance to the *Eastmond* test. For example, further work is needed in defining intellectual privacy and its broader social value, perhaps informed in part by intellectual privacy's value to the objectives of copyright.

71. Lisa M. Austin, "Is Consent the Foundation of Fair Information Practices? Canada's Experience under PIPEDA" (November 2005) *University of Toronto, Legal Studies Research Paper No. 11–05* Available at SSRN: http://ssrn.com/abstract=864364: 43.