THE NEXUS OF COPYRIGHT AND INTELLECTUAL PRIVACY

Alexander Dugan Cameron

Thesis submitted to the
Faculty of Graduate and Postdoctoral Studies
in partial fulfillment of the requirements
for the Doctor of Laws (LL.D.) degree.

Common Law Section
Faculty of Law
University of Ottawa

© Alexander Dugan Cameron, Ottawa, Canada, 2012

ACKNOWLEDGEMENTS

For their steadfast and complete support, I am eternally grateful to my amazing wife and children. Without them, and without the support and encouragement of our families (and especially my mother), this project would not have been completed.

I am profoundly grateful to my supervisor, the exceptional Dr. Ian Kerr, Canada Research Chair in Ethics, Law and Technology, for always inspiring me, for his unfailing enthusiasm, personal encouragement and feedback, and for the tremendous support, friends, opportunities and experiences I was privileged to gain through the inter-disciplinary research project of which he was Principle Investigator: “On the Identity Trail: Understanding the Importance and Impact of Anonymity and Authentication in a Networked Society” (www.anonequity.org).

My most sincere thanks to Teresa Scassa and Jane Bailey for providing me with their insightful comments on drafts of this dissertation, particularly on short notice during the home stretch. Thank you also to Michael Geist, Daniel Gervais, and Philippa Lawson for their teaching, assistance and inspiration which at different times and in different ways contributed to this dissertation.

I also wish to acknowledge and express deep thanks for the opportunities, support and assistance that I received in connection with this dissertation from the Social Sciences and Humanities Research Council, the University of Ottawa Faculty of Law, the Law Foundation of British Columbia, the Ontario Research Network for Electronic Commerce, Fasken Martineau DuMoulin LLP, the Office of the Privacy Commissioner of Canada, the Samuelson-Glushko Canadian Internet Policy & Public Interest Clinic, and the Electronic Privacy Information Center.

ABSTRACT

For nearly three centuries following the enactment of the world's first modern copyright statute, neither copyright law nor copyright holders interfered with individuals' intellectual privacy—individuals' freedom to access and enjoy creative works anonymously or in private. Neither *Rights of Man*, nor *The Clockmaker* 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.

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 copyright works—the centuries-old relationship between copyright holders and individuals became strained. In particular, the relationship between copyright law, copyright holders and individuals' intellectual privacy came into tension.

This dissertation proffers a description of intellectual privacy and, without making empirical claims, asks whether diminishing it in the name of copyright holders' interests will lead to the impoverishment of the very copyright kingdoms that we purport to be protecting in so doing. In response to this question, this dissertation tests the hypothesis that individuals' intellectual privacy is an essential component of copyright as a consistent and unified whole (even if it may mean that some individual copyright holders are not improved) and that copyright law can and should explicitly internalize protection of intellectual privacy. Ultimately, this dissertation formulates principles and five basic recommendations for rules to account for intellectual privacy within the legal concept of copyright. This dissertation concludes with a look ahead to further work to be done in the area.

CONTENTS

ACKNOWLEDGEMENTS.....	i
ABSTRACT	ii
CONTENTS	iii
ABBREVIATIONS.....	vii
CHAPTER 1: INTRODUCTION	1
I. Mise en scène	3
II. Implications for Intellectual Privacy	12
III. The Search for Solutions	19
IV. Understanding Intellectual Privacy through Books.....	24
V. Overview of Contents.....	34
CHAPTER 2: INTELLECTUAL PRIVACY	38
I. Introduction	38
II. Privacy	47
A. The Canadian Charter of Rights and Freedoms.....	51
B. Common Law and Civil Law	58
C. Privacy Legislation.....	67
1. First Generation: Statutory Torts	67
2. Second Generation: Data Protection Legislation.....	69

3.	Third Generation: Sector-Specific Laws	72
III.	What is Intellectual Privacy?	76
A.	Defining Intellectual Privacy	76
B.	Reading, Writing and Thought	84
C.	Values that are interrelated with Intellectual Privacy	92
IV.	Some Limits of Intellectual Privacy	103
CHAPTER 3: CONTEMPORARY CONFLICT BETWEEN COPYRIGHT AND INTELLECTUAL PRIVACY		111
I.	Technology	112
A.	TPMs and RMI	113
B.	DRM	117
C.	Impact of DRM on Intellectual Privacy	123
II.	Law	134
A.	Contracts and copyright	135
B.	Anti-circumvention and anti-device laws	142
C.	Internet service provider (ISP) liability	148
D.	Copyright litigation	155
III.	Intermediaries	171
IV.	Conclusions	185
CHAPTER 4: THE NEXUS OF COPYRIGHT AND INTELLECTUAL PRIVACY		186
I.	The Purposes of Copyright	188
A.	Théberge	190
B.	CCH Canadian	192
C.	SOCAN v. CAIP	195

D.	Robertson and Kraft.....	197
E.	Conclusions.....	199
II.	Links Between Copyright and Intellectual Privacy	203
A.	Right of First Publication	204
B.	Moral Rights	211
C.	The Private Sphere	215
1.	The Traditional Position.....	215
2.	Addressing Privacy	219
D.	Related Protections	221
III.	Contemporary Copyright Must Account for Intellectual Privacy	224
A.	Technological Developments Require a Response.....	225
B.	Copyright Objectives Support Addressing Intellectual Privacy.....	228
CHAPTER 5: ACCOUNTING FOR INTELLECTUAL PRIVACY WITHIN COPYRIGHT		234
I.	Lessons from data protection law.....	237
A.	Surveillance and Related Jurisprudence under <i>PIPEDA</i>	239
1.	Personal Information.....	246
2.	Knowledge and Consent.....	248
B.	Is DRM Monitoring an Appropriate Purpose?	252
1.	Is monitoring necessary to meet a specific need?	254
2.	Is monitoring likely to be effective in meeting the need?	259

3.	Is the loss of privacy proportional to the benefit gained?	261
4.	Is there a less privacy-invasive way of achieving the same end?	268
C.	Conclusions	269
II.	Recent Proposals for Statutory Reform	273
A.	Levies Redux	273
B.	Proposed Amendments to the Copyright Act	276
III.	Imagining Intellectual Privacy Rules in Copyright Reform Statutes	281
IV.	Conclusions	293
	CONCLUSIONS	294

ABBREVIATIONS

ACM	Association for Computing Machinery
ALA	American Library Association
ALAI	Association littéraire et artistique internationale
CASL	Canada's Anti-Spam Law
CIPPIC	Canadian Internet Policy and Public Interest Clinic
CRIA	Canadian Recording Industry Association
CRTC	Canadian Radio and Telecommunications Commission
CSA	Canadian Standards Association
DRM	Digital Rights Management
EFF	Electronic Frontier Foundation
EPIC	Electronic Privacy Information Center
EU	European Union
INDICARE	Informed Dialogue about Consumer Acceptability of DRM Solutions in Europe
ISP	Internet service provider
IVIR	Institute for Information Law
MPAA	Motion Picture Association of America
OECD	Organisation for Economic Co-operation and Development
OPC	Office of the Privacy Commissioner of Canada
<i>PIPEDA</i>	Personal Information Protection and Electronic Documents Act
P2P	Peer to peer
RIAA	Recording Industry Association of America

RMI	Rights Management Information
SCC	Supreme Court of Canada
TC	Trusted Computing
TPM	Technological Protection Measure

CHAPTER 1:

INTRODUCTION

This dissertation¹ proffers a description of intellectual privacy—individuals’ freedom to access and enjoy creative works² anonymously or in private—and, without making empirical claims, asks whether diminishing it in the name of copyright holders’ interests will lead to the impoverishment of the very copyright kingdoms that we purport to be protecting in so doing.³ In

¹ The views expressed in this dissertation are the author’s own. Portions of this chapter are derived in part from Alex Cameron, “Learning from Data Protection Law at the Nexus of Copyright and Privacy” in Ian Kerr, Valerie Steeves & Carol Lucock, eds, *Lessons from the Identity Trail: Anonymity, Privacy and Identity in a Networked Society* (New York: Oxford University Press, 2009) 43 [Cameron, “Learning from Data Protection Law”].

² A ‘work’ is a term of art. In Canada, many forms of works are protected by copyright: literary, dramatic, musical, and artistic works, including paintings, drawings, maps, charts, plans, photographs, engravings, and sculptures. See *Copyright Act*, RSC 1985, c C-42 s 2.

³ The use of the word ‘access’ in this paragraph is not intended to argue in favour of a guarantee of access to works. The focus herein is on the privacy-related conditions under which access should take place. In addition, this definition of intellectual privacy is purposefully general. Chapters 2 and 3 build a fuller exposition of the concept with reference to the literature: see e.g. Julie Cohen, “DRM and Privacy” (2003) 18 Berkeley Tech LJ 575 [Cohen, “DRM and Privacy”] (“[Intellectual privacy] concerns the extent of ‘breathing space,’ both metaphorical and physical, available for intellectual activity [and] extends both to information about intellectual consumption and exploration

response to this question, this dissertation tests the hypothesis that individuals' intellectual privacy is an essential component of copyright as a consistent and unified whole (even if it may mean that some individual copyright holders are not improved) and that copyright law can and should explicitly internalize protection of intellectual privacy. Ultimately, this dissertation formulates principles and five basic recommendations for rules to account for intellectual privacy within the legal concept of copyright. This dissertation asserts that the principles and rules described herein have been lacking in copyright before now and that they are an essential component of copyright as a consistent and unified whole.⁴

and to the physical and temporal circumstances of intellectual consumption within private spaces" at 576).

- ⁴ The description of the goals of this dissertation is inspired in part by the following passages from Lyman R Patterson, *Copyright in Historical Perspective* (Nashville: Vanderbilt University Press, 1968) at 222:

Copyright can most usefully be viewed as a legal concept—a series of ideas formulated and directed to a common end. [...] The general ideas are principles expressing the ends to be achieved; the specific ideas are the rules, expressing the means of achieving those ends. The principles are directed to the purposes to be served, the rules are directed to the resolution of problems in order to achieve those purposes. Legal concepts are thus ideally formulated in terms of purposes to be achieved and problems to be resolved.

The purposes, however, are not always clearly defined, and the problems are not always agreed upon. As the history of copyright illustrates, purposes and problems vary according to whose interest is being served. Moreover, they change with new developments. The changes, however, do not necessarily result in the appropriate development of rules. Almost certainly they do not if the principles have not been properly formulated, for of the two groups of ideas, principles and rules, principles are by far the more important. It is the choice of principles that determines whether a legal concept is to have the degree of

I. Mise en scène

For nearly three centuries following the enactment of the world's first modern copyright statute,⁵ neither copyright law nor copyright holders interfered with individuals' intellectual privacy. Neither *Rights of Man*,⁶ nor *The Clockmaker*⁷ 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.⁸

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, reading at home, visiting a library or attending a public performance. These pre-digital forms of access to and enjoyment of creative works usually afforded individuals a high degree of intellectual privacy. Once an individual had purchased or otherwise accessed a copy of a work, her relationship with the copyright holder or the distributor of the work ended; it was normally up to the individual to determine

consistency necessary for a unified whole, or whether it is to consist primarily of a series of fragmented rules.

⁵ *Copyright Act*, 1710 (UK), 8 Ann, c 19 [*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 & Stanley W Lindberg, *The Nature of Copyright: A Law of Users' Rights* (Athens, Georgia: University of Georgia Press, 1991) at 42, n 22.

⁶ Thomas Paine, *Rights of Man* (London: J S Jordan, 1791).

⁷ Thomas Chandler Haliburton, *The Clockmaker, or, The Sayings and Doings of Samuel Slick, of Slickville* (Halifax: J Howe, 1836).

⁸ 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 libelous" work. See generally Thomas Paine, *The Political Writings of Thomas Paine: To which is Prefixed a Brief Sketch of the Author's Life*, vol 1 (Charlestown: G Davidson, 1824) at xi.

how, when and under what conditions she enjoyed the work, subject of course to the terms of copyright law.⁹ The condition of intellectual privacy inherent in these forms of access was sometimes bolstered by convention and legal rules, including protections against disclosure of library patrons' borrowing records to the state.¹⁰

Additionally and in part because of the fact that individuals had limited means to reproduce and disseminate works in 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.¹¹ Even if copyright holders or others had been interested in collecting detailed information about individuals'

⁹ See generally Jacques de Werra, "The Legal System of Technological Protection Measures under the WIPO Treaties, the Digital Millennium Copyright Act, the European Union Directives and other National Laws (Japan, Australia)" (Paper delivered at the Association littéraire et artistique internationale (ALAI) Congress 2001: Adjuncts and Alternatives to Copyright, June 2001), online: ALAI <http://www.alai-usa.org/2001_conference/Reports/dewerra.doc> ("...in the present world of tangible objects, if the user buys a book in a bookstore, she owns it and can exclusively decide on its future use, this private use being not submitted to any further payment or conditions imposed by the copyright owners" at 14).

¹⁰ See e.g. *The Library Records Confidentiality Act*, 75 ILCS 70/1 (1984). See generally Herbert N Foerstel, *Surveillance in the Stacks: The FBI's Library Awareness Program* (Westport: Greenwood Press, 1991).

¹¹ See generally Daniel Gervais, "Use of Copyright Content on the Internet: Considerations on Excludability and Collective Licensing" in Michael Geist, ed, *In the Public Interest: The Future of Canadian Copyright Law* (Toronto: Irwin Law, 2005) 517 at 523 [Geist, *In the Public Interest*]. Chapter 4 reviews some of the historical features of copyright relevant to this dissertation.

access to and use of creative works, they had no efficient practical means to do so.¹²

The foregoing characterization of the pre-digital world is not meant to suggest that this dissertation is concerned only with the collection of information about individuals' access to and enjoyment of works, a practice which principally implicates informational privacy. The focus herein is on a concept of intellectual privacy, as distinct from other forms of privacy, including informational privacy. Informational privacy is principally concerned with individuals' claim to control whether, how and what information about them is collected, used and disclosed by others.¹³ Informational privacy is certainly at stake in

¹² *Ibid.* See also Ross Anderson, *Security Engineering: A Guide to Building Dependable Distributed Systems*, 2d ed (Indianapolis: Wiley, 2008) at 414:

In theory, there is no compelling reason why [copyright and privacy] should be in conflict, and in the pre-electronic world, they usually weren't. Copyright was protected by the cost of small-scale duplication; it was simpler and cheaper to buy a book or a record than to make a single copy, and people who made large numbers of copies could usually be tracked down and prosecuted. The cost barrier to copying was eroded significantly by the photocopier and the cassette recorder, but they didn't change the basic economics.

Of course, in certain circumstances copyright holders could obtain a court order to compel disclosure of some forms of information about individuals' access to and use of creative works, usually as part of a civil action for copyright infringement, and law enforcement could obtain a warrant for such information in the course of a criminal investigation.

¹³ See e.g. *R v Tessling*, 2004 SCC 67 at para 23, citing Alan Westin, *Privacy and Freedom* (New York: Atheneum, 1970) ("Privacy is the claim of individuals, groups, or institutions to determine for themselves when, how, and to what extent information about them is communicated to others" at 7). See also *R v Dymnt*, [1988] 2 SCR 417 at paras 17, 20; Arthur R Miller, *The Assault on Privacy: Computers, Data Banks, and Dossiers* (Ann Arbor: University of Michigan Press, 1971) at 25; Julie Cohen, "Examined Lives: Informational Privacy and the Subject as Object" (2000) 52 *Stan L Rev* 1373 [Cohen, "Examined Lives"] (discussing conceptions of informational privacy but

many of the examples of tension between copyright and intellectual privacy discussed herein. It can also be a means to achieve intellectual privacy and may contribute to our understanding of whether and how intellectual privacy ought to be protected.¹⁴ As argued in Chapter 2, however, intellectual privacy encompasses an important set of interests distinct from informational privacy and other notions of privacy. While it must be acknowledged that there is a close relationship between informational privacy and intellectual privacy and that informational privacy (at least in the form that it is protected under data protection laws in Canada) could do a lot more to address intellectual privacy,¹⁵ it is asserted in this dissertation that informational privacy does not capture all that is captured by the concept of intellectual privacy as described herein.¹⁶ Foreshadowing some of discussion in Chapter 2 of this dissertation, Richards puts the point as follows:

noting that “privacy theory and privacy rhetoric do not know quite what to do with the notion of ‘informational privacy’” at 1375); Daniel J Solove & Marc Rotenberg, *Information Privacy Law* (New York: Aspen, 2003) at 184-92. Fair information practices are based on informational privacy. See Organization for Economic Co-operation and Development (OECD) Directorate for Science, Technology and Industry, *Guidelines on the Protection of Privacy and Transborder Flows of Personal Data* (Paris: OECD Publications, 1980) [OECD Guidelines]; Canadian Standards Association (CSA), *Model Code for the Protection of Personal Information* (CSA Publications, 1996) [CSA Model Code]. *Personal Information Protection and Electronic Documents Act*, SC 2000 c 5 [PIPEDA] (incorporating the CSA Model Code); UK, *Data Protection Act 1998*, c 29.

¹⁴ The concept of intellectual privacy presented in this dissertation will be built incrementally in Chapters 2 through 4.

¹⁵ See Chapter 5.

¹⁶ See generally Neil Richards, “Intellectual Privacy” (2008) 87 Tex L Rev 387 (providing four examples of cases involving the surveillance of intellectual activity where “the traditional privacy paradigm was applied, and as a result the special issues of intellectual privacy were largely missed” and asserting that “[t]he failure to appreciate the special nature of intellectual privacy (even by privacy advocates) resulted in discussions and outcomes that minimized the critical cognitive-liberty issues at stake” at 390-91).

For run-of-the-mill issues of personal information, even embarrassing personal information, the traditional paradigm may be a reasonable way for the law to deal with problems of information collection and use. But when ... businesses are tracking and analyzing what we read, these activities menace our processes of cognition and our freedoms of thought and speech. ...

Intellectual privacy is different from other conceptions of privacy, such as those that protect individuals from the emotional harm of information disclosure. It is not concerned with remedying tort injury, but rather with the way our cognitive processes, and ultimately our public discourse, are constituted. ... Intellectual privacy involves only a fraction of the many issues we might think of as involving “privacy,” but this fraction of issues is discrete and worthy of separate treatment.¹⁷

Contrasted against the foregoing 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 copyright works—the centuries-old relationship between copyright holders and individuals became strained.¹⁸ In particular, the relationship between copyright law, copyright holders and individuals’ intellectual privacy came into tension. 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’

¹⁷ *Ibid* at 391-92.

¹⁸ 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. However, it was not 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 individuals’ use of personal computers and the Internet.

borrowing records.¹⁹ Similar protections have existed for some time in respect of individuals' video rental records and bookstore purchases.²⁰ 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.²¹ Although libraries continue to stand by privacy in the digital age, going so far as to engage in advocacy²² and to develop privacy

¹⁹ See *supra* note 10 and accompanying text. See also American Library Association (ALA), "Policy on Confidentiality of Library Records", Adopted January 20, 1971 by the American Library Association Council; amended July 4, 1975; July 2, 1986 [ALA, "Policy on Confidentiality of Library Records"].

²⁰ See e.g. *Video Privacy Protection Act of 1988*, 18 USC § 2710 [*Video Privacy Protection Act*] (designed to prevent the improper disclosure of video tape rental or sale records). See generally Associated Press, "Court Overturns Bookstore Ruling", *Wired Magazine* (9 April 2002), online: WIRED <<http://www.wired.com/news/privacy/0,1848,51667,00.html>>; Daniel J Solove, "Digital Dossiers and the Dissipation of Fourth Amendment Privacy" (2002) 75 S Cal L Rev 1083; Phillip Taylor, "Kramerbooks declares victory in subpoena battle", *Freedom Forum* (22 June 1998), online: Freedom Forum <<http://www.freedomforum.org/templates/document.asp?documentID=9736>> (reporting on Kramerbooks' opposition to Kenneth Starr's subpoena of books purchased by Monica Lewinsky during the Lewinsky-Clinton scandal).

²¹ It is notable, however, that public libraries saw substantial increases in circulation and new library-card applications in recent years. Freakonomics, "The Public Library Renaissance" *New York Times* (7 January 2009), online: NYT.com <<http://freakonomics.blogs.nytimes.com/2009/01/07/the-public-library-renaissance>>. Libraries are also seeking new ways to attract patrons, including lending humans: Fan Yee Suen, "'Human lending' to prove libraries aren't just book depots" *CTV News.ca* (28 August 2011), online: CTV <<http://toronto.ctv.ca/servlet/an/plocal/CTVNews/20110827/new-surrey-library-to-lend-living-books-110828/20110828/?hub=TorontoNewHome>>.

²² See e.g. ALA Office for Intellectual Freedom Privacy Revolution website, online: ALA <<http://www.privacyrevolution.org>>. See also James Waldo, Herbert Lin & Lynette I Millett, *Engaging privacy and information technology in a digital age* (Washington: National Academies Press, 2007) ("For libraries, privacy is seen primarily as an instrumental good, but one that has been discussed and thought about to such an extent that the members of the American Library Association have become fierce advocates for the privacy of their patrons" at 236).

guidelines²³ for publishers of electronic resources that the libraries license for individuals, we cannot rely on only our libraries to protect our intellectual privacy; we must decide more broadly whether and how to preserve the values of intellectual privacy in the digital era, including whether intellectual privacy has a place in copyright law.²⁴

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 riders on ‘the Clapham omnibus’ a virtually effortless means to, for example, 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.²⁵ The most widely-known example of this activity is

²³ See International Coalition of Library Consortia (ICOLC), “Privacy Guidelines for Electronic Resources Vendors” (July 2002), online: Yale University <<http://www.library.yale.edu/consortia/2002privacyguidelines.html>>. These ICOLC principles are supported, for example, by ABC-CLIO, a California book publisher. See ABC-CLIO, “Product Privacy Policy”, online: ABC-CLIO <http://www.abc-clio.com/privacy_popup.html>.

²⁴ 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) at 191 [Lessig, *Code version 2.0*].

²⁵ The term “riders” is used here intentionally to take the emphasis off the use of gender in the well-known phrase ‘the man on the Clapham omnibus.’ The phrase is a legal fiction that refers to an ordinary, reasonable person. ‘The man

peer-to-peer (P2P) file sharing of music using the products and services offered by, among others, the original Napster service.²⁶

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 implicated most profoundly. For example, in order to pursue the opportunities and to mitigate the threats of digital networks, a number of copyright holders and others who distribute copyright works turned to technological means to attempt to control individuals' access to and enjoyment of copyright works. 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.²⁷ DRM is a kind of "electronic security guard."²⁸ DRM technologies used to control a

on the Clapham omnibus' was first adopted in legal circles in *McQuire v Western Morning News*, [1903] 2 KB 100 at 109. For a contemporary Canadian version of the fiction using the female gender, see Yves-Marie Morissette, "The Exclusion of Evidence under the Canadian Charter of Rights and Freedoms: What to Do and What Not to Do" (1984) 29 McGill LJ 521 ("A convenient and longstanding legal fiction exists for the purposes of judicial dialectics: the reasonable man, whether it be the man on the Clapham omnibus or, perhaps today in Canada, the career-woman on the Voyageur bus" at 538).

²⁶ 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).

²⁷ Although a fuller account of DRM, technological protection measures (TPMs), and rights management information (RMI) is contained in Chapter 3, it suffices for the purposes of this chapter to reference a general definition of DRMs.

²⁸ Alex Cameron, "Infusing Privacy Norms in DRM - Incentives and Perspectives from Law" in Yves Deswarte et al, eds, *Information Security Management, Education and Privacy*, IFIP 18th World Computer Congress, TC11

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 tablet.

Conditions that could be enforced through DRM technologies are limited virtually by the imagination, including, for example, 'do not copy more than five times,' 'do not modify,' 'do not print,' 'do not save as a different file format,' or 'listen only once.' Some business models depend on DRM by virtual necessity as a result of licenses negotiated between retailers and rights holders or as a result of the nature of the business model, including subscription or rental services.²⁹ For example, an online movie rental service might permit individuals to download a movie and watch it an unlimited number of times within 30 days of the download date. DRM is required by virtual necessity in such a business model because the model depends on the movie being inaccessible after the 30 day period expires. DRM technologies continue to evolve and are used by contemporary copyright holders and others in association with many different forms of works.³⁰

19th International Information Security Workshops, 22-27 August 2004, Toulouse, France (Berlin: Kluwer, 2004) ("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" at 2) [Cameron, "Infusing Privacy Norms in DRM"].

²⁹ See Lucie Guibault et al, "Study on the Implementation and Effect in Member States' Laws of Directive 2001/29/EC on the Harmonization of Certain Aspects of Copyright and Related Rights in the Information Society" (February 2007) at 15, online: Institute for Information Law (IVIR) <http://www.ivir.nl/publications/guibault/Infosoc_report_2007.pdf>. See also Steve Jobs, "Thoughts on Music" (6 February 2007), online: Apple <<http://www.apple.com/hotnews/thoughtsonmusic/>>.

³⁰ For a review and privacy analysis of 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

II. Implications for Intellectual Privacy

It is perhaps not surprising that DRM technologies have sparked controversy on a number of fronts.³¹ Among other examples discussed in Chapter 3, DRM technologies are relevant for the purpose of this dissertation because many forms of DRM are emblematic of the tension between copyright and intellectual privacy experienced to date in the digital age. In ostensibly exploiting copyright works and preventing copyright infringement, many DRM technologies, and the licensing (i.e. contracting) practices that they enable, depend in part on identifying and tracking copyright works, as well as the individuals who access and use them.³² Many forms of DRM use a monitoring mechanism as a component of controlling access to and use of creative works.³³

Under Canadian Privacy Law" (2007)
<http://www.cippic.ca/uploads/CIPPIC_Report_DRM_and_Privacy.pdf>
[CIPPIC, "Digital Rights Management and Consumer Privacy"]. The author contributed to this study and report.

³¹ See generally Natali Helberger et al, "Digital Rights Management and Consumer Acceptability, A multi-disciplinary discussion of consumer concerns and expectations: State of the Art Report" (December 2004), online: Informed Dialogue about Consumer Acceptability of DRM Solutions in Europe (INDICARE) <http://www.indicare.org/tiki-download_file.php?fileId=60> [Helberger et al, "INDICARE 2004"]; Natali Helberger et al, "Digital Rights Management and Consumer Acceptability, A Multi-Disciplinary Discussion of Consumer Concerns and Expectations State of the Art Report - First Supplement" (May 2005), online: INDICARE <http://www.indicare.org/tiki-download_file.php?fileId=111> [Helberger et al, "INDICARE 2005"]. One of the important issues raised by DRM relates to competition law and policy. See e.g. Alex Cameron & Robert Tomkowicz, "Competition Policy and Canada's New Breed of 'Copyright' Law" (2007) 52 McGill LJ 291.

³² See generally Ian R Kerr, Alana Maurushat & Christian S Tacit, "Technological Protection Measures: Part I — Trends in Technical Protection Measures and Circumvention Technologies" (Ottawa: Department of Canadian Heritage, 2003) [Kerr, Maurushat & Tacit, "TPMs Part I"] at § 5.2.2:

In many cases, DRM operation is fundamentally premised on a diminishment of individuals' intellectual privacy because through the monitoring of and collection of information³⁴ about individuals access to and use of copyright works DRM reduces or eliminates individuals' ability to access and enjoy copyright works anonymously or in private. Although there are many examples of this diminishment, a number of which are discussed in Chapter 3, it is worth briefly noting one now for demonstrative purposes.

eReader offers a catalogue of over 37,000 electronic books for sale on its website.³⁵ An individual downloads the purchased book,

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 services, the tremendous potential for acquisition of personal information also gives rise to serious privacy concerns. [footnotes and citations omitted]

See also Ian Kerr, Alana Maurushat, & Christian S. Tacit, "Technical Protection Measures: Part II – The Legal Protection of TPMs" (2002), online: Heritage Canada <http://www.pch.gc.ca/progs/ac-ca/progs/pda-cpb/pubs/protectionII/index_e.cfm> [Kerr, Maurushat & Tacit, "TPMs Part II"]; Lee Bygrave, "Digital Rights Management and Privacy—Legal Aspects in the European Union" in Eberhard Becker et al, eds, *Digital Rights Management—Technological, Economic, Legal and Political Aspects* (Berlin: Springer-Verlag, 2003) 418; Deirdre K Mulligan, John Han & Aaron J Burstein, "How DRM-based content delivery systems disrupt expectations of 'personal use'" in Joan Feigenbaum & Tomas Sander, eds, *Proceedings of the 2003 ACM workshop on Digital rights management* (New York: ACM Press, 2003) 77.

³³ See e.g. Kerr, Maurushat & Tacit, "TPMs Part I", *ibid* at § 5.2.2.

³⁴ This highlights the interrelationship between intellectual privacy and informational privacy.

³⁵ eReader, "ebooks for your iPhone, Windows Mobile Pocket PC and Smartphone, Palm Treo and Centro or Symbian Mobile Phones - Over 37,000 Titles and counting!", online: eReader <<http://www.ereader.com/>>.

installs the eReader software, enters her password—which is in fact her credit card number³⁶—to unlock the book, and is then able to read it.³⁷ 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 [eReader] site for you.³⁸

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 information as part of its interactions with its customers and that it transmits data during operation of the eReader software.³⁹ Data collected could conceivably include a list of book searches or book titles purchased. However, to gain an appreciation of the full scope of information that the software could be collecting and reporting back to eReader, consider that the software “eReader Pro for Windows” is capable of the following functions:

³⁶ eReader, “Frequently Asked Questions”, online: eReader <<https://secure.ereader.com/ereader/help/faq.htm#supportFAQ>>. This use of the credit card number as a password has been criticized by CIPPIC. See CIPPIC, “Digital Rights Management and Consumer Privacy”, *supra* note 30 at 35.

³⁷ eReader, “Installation: Opening an eBook”, online: eReader <<http://www.ereader.com/ereader/help/ereader/guide/install.htm>>. See generally CIPPIC, “Digital Rights Management and Consumer Privacy”, *ibid*.

³⁸ eReader, “Privacy Policy”, online: eReader <<http://www.ereader.com/ereader/privacy.htm>>. See also CIPPIC, “Digital Rights Management and Consumer Privacy”, *ibid* at 47.

³⁹ CIPPIC, “Digital Rights Management and Consumer Privacy”, *ibid* at 61.

...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.⁴⁰

Subject to considerations about whether meaningful consent was obtained from affected individuals, intellectual 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.⁴¹

Of course, not all forms of DRM are inherently privacy-invasive. A number of commentators have noted that DRM design need not involve detailed monitoring or the collection of personal information in order to prevent copyright infringement.⁴² In addition, a number of commentators have suggested that DRM

⁴⁰ eReader, "eReader Pro for Windows Software", online: eReader <http://www.ereader.com/ereader/software/product/15009_pro_win.htm>.

⁴¹ See generally Electronic Frontier Foundation (EFF), *Updated and Corrected: E-Books Buyer's Guide to Privacy*, (6 January 2010), online: EFF.org <<http://www.eff.org/deeplinks/2010/01/updated-and-corrected-e-book-buyers-guide-privacy>> (reviewing the privacy policies of a number of e-book readers and services).

⁴² See e.g. Claudine Conrado, Milan Petkovic & Willem Jonker, "Privacy-Preserving Digital Rights Management" in Milan Petkovic & Willem Jonker, eds, *Secure Data Management: Vldb 2004 Workshop, Sdm 2004, Toronto, Canada, August 30, 2004, Proceedings* (New York: Springer, 2004) 83 at 84. For a discussion of such proposals, see Cameron, "Infusing Privacy Norms in DRM", *supra* note 28; Ian Kerr "If Left to their own Devices: How DRM and Anti-circumvention Laws Can Be Used to Hack Privacy", in Geist, *In the Public Interest*, *supra* note 11 at 183-85 [Kerr, "If Left to their own Devices"].

collides with privacy only when it strays beyond copyright protection.⁴³

As the eReader example illustrates, there are a variety of purposes for which DRM might monitor access to and use of works, not the least of which are marketing purposes. On a sliding scale ranging from purposes that are relatively close to the heart of copyright law, to purposes that are further from and arguably outside the typical scope of copyright law, the following list is one way of thinking about the kinds of purposes and motives that might underlie DRM monitoring in any given case:

DRM monitoring can help prevent copyright infringement;

Where copyright infringement does occur, DRM monitoring can help facilitate copyright enforcement action because it collects information about the infringement;

DRM monitoring can increase the number of discrete uses of a work that can be exploited;⁴⁴

⁴³ See e.g. Mulligan, Han & Burstein, *supra* note 32; Guibault et al, *supra* note 29 at 15:

The more DRM solutions move from copyright protection in the narrow sense to the management of digital contents in the broader sense, the more additional, non-copyright-law-related concerns of consumers are expressed. Examples are privacy concerns, concerns regarding user-friendliness, interoperability, sustainability, and security issues.

Based on the discussion in the remaining passages of this part and in Chapter 3 herein, it is certainly arguable that DRM's implications for intellectual privacy are more widespread or aggravated the further that DRM practices stray from the protection of copyright from unauthorized access or use (e.g. to create detailed profiles of individuals' preferences for marketing or other purposes). However, this dissertation does not depend on that point. It is asserted herein that DRM monitoring for the purpose of detecting, preventing or investigating copyright infringement equally implicates intellectual privacy.

DRM monitoring can facilitate and enforce compliance with licenses that delineate the uses that an individual can make of a work;

DRM monitoring can be a valuable source of information to help a copyright holder better market and exploit a work, or other works; and

DRM monitoring can be a valuable source of information for marketing to individuals more generally, both by the copyright holder and by any other entity that the information is disclosed to.

Any number of these purposes, or all of them, may be a source of tension with intellectual privacy in a given case. Some commentators have argued that the desire to participate in new markets for trading in personal information, as reflected in the last two points in the list above, is potentially one of the most significant driving forces behind DRM monitoring.⁴⁵ It must be acknowledged that such motives, not copyright law *per se*, may in some cases be the primary source of tension with intellectual

⁴⁴ Barlow introduced us to the image 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.” John Perry Barlow, “Life, Liberty and the Pursuit of Copyright?” *The Atlantic* (17 September 1998), online: The Atlantic Online <<http://www.theatlantic.com/unbound/forum/copyright/barlow2.htm>>.

⁴⁵ Such arguments are consistent with the notion, described in this chapter, that we are at a unique point in the history of copyright and intellectual privacy. For discussion of how copyright holders and others in the copyright distribution chain can be interested in DRM monitoring because it allows them to participate in new markets for personal information, see Mulligan, Han & Burstein, *supra* note 32 at 82-83; Cameron, “Infusing Privacy Norms in DRM”, *supra* note 28 at § 2; Julie Cohen, “A Right to Read Anonymously: A Closer Look at ‘Copyright Management’ in Cyberspace” (1996) 28 Conn L Rev 981 [Cohen, “A Right to Read Anonymously”]. See also Guibault et al, *supra* note 29.

privacy. Since the activities and the solutions proposed in this dissertation center around individuals' access to and enjoyment of copyright works, however, this dissertation characterizes the tension as one between copyright and intellectual privacy.

eReader provides one example of the kinds of conflict that can arise between copyright and intellectual privacy. Although this specific example and others like it may be resolved, their resolution is not determinative of the overarching questions that they raise about the nexus 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 a dangerous one in need of repair or redesign.

Through the use of many forms of DRM and as a result of other developments discussed in Chapter 3, 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 copyright works. These conditions are the norm facing individuals wishing to access and enjoy many modern forms of digital works. Apple's leading iTunes service, to take another example, at one time required individuals to furnish and maintain accurate personal information with Apple, failing which Apple could terminate services:

7. Your Information. You agree to provide accurate, current, and complete information required to register with the Service and at other points as may be required in the course of using the Service ("Registration Data"). You further agree to maintain and update your Registration Data as required to keep it accurate, current, and complete. Apple may terminate your rights

to any or all of the Service if any information you provide is false, inaccurate or incomplete. [...]⁴⁶

Tension 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 creative works. Although it need not be so, to date the consequence of this conflict has been a diminishment of individuals' intellectual privacy.⁴⁷ Should conflict between copyright and intellectual privacy continue on its current path, we may be left with little or no room to travel our vibrant copyright kingdoms anonymously or in private.⁴⁸

III. The Search for Solutions

It is possible that the diminishment of intellectual privacy through the use of some forms of DRM (and by other means discussed in Chapter 3) will be halted or reversed. Any number of changes in

⁴⁶ Apple, "iTunes Store Terms of Service", online: Apple <<http://www.apple.com/legal/itunes/us/service.html>>. In addition, consider the following example from CMT.com, where individuals can browse, listen to and purchase country music and country music videos: "All users of the Site are required to provide true, current, complete and accurate Personal Information... As a registered user, you acknowledge, understand and hereby agree that you are giving us your *consent to track your activities* and your use of the Site and its functions and features..." [emphasis added]. Country Music Television (CMT), "CMT.com Privacy Statement," online: CMT <<http://www.cmt.com/interact/terms/privacy.jhtml>>.

⁴⁷ Chapter 3 reviews a number of contemporary examples.

⁴⁸ See e.g. Graham Greenleaf, "IP, Phone Home: Privacy as Part of Copyright's Digital Commons in Hong Kong and Australian Law" in Lawrence Lessig, ed, *Hochelaga Lectures 2002: The Innovation Commons* (Hong Kong: Sweet & Maxwell Asia, 2003) [Greenleaf, "IP Phone Home"] (suggesting that technological surveillance mechanisms may "bring about the end of the anonymity of reading" at 14).

technology, markets and regulation may influence the course of intellectual privacy in one direction or another.⁴⁹ There are, for example, a number of recent indications that DRM has been dropped by a number of organizations in connection with music downloads and audio books,⁵⁰ though it is not clear that enhanced intellectual privacy will necessarily result from such developments.⁵¹

Differences have also emerged between different groups of copyright holders and between copyright holders and authors as to

⁴⁹ Professor Daniel Gervais introduced the author to this “technopolicy triangle”. See Daniel J Gervais, “The Price of Social Norms: Towards a Licensing Regime for File-Sharing” (2005) 12 J Intell Prop L 39 [Gervais, “Price of Social Norms”].

⁵⁰ See e.g. Yinka Adegoke, “Sony BMG to drop copy protection for downloads” Reuters (7 January 2008), online: cNet < http://news.cnet.com/Sony-BMG-to-drop-copy-protection-for-downloads/2100-1027_3-6224807.html>; Richard Wray, “Penguin audiobooks to be free of copyright protection” The Guardian (4 March 2008), online: The Guardian <<http://www.guardian.co.uk/technology/2008/mar/04/digitalmusic.booksnews>>; Fred von Lohmann, “DRM for Streaming Music Dies a Quiet Death” EFF.org (15 August 2008), online: <<http://www.eff.org/deeplinks/2008/08/drm-quietly-dies-streaming-music>>; Ethan Smith & Yukari Iwakani Kane, “Apple Changes Tune on Music Pricing” *Wall Street Journal* (7 January 2009), online: WSJ <<http://online.wsj.com/article/SB123126062001057765.html>> (reporting that Apple plans to discontinue the use of copy protection from all of the songs in its digital store). See also Ed Felten, “DRM In Retreat” *Freedom to Tinker* (January 22, 2009), online: Freedom to Tinker <<https://freedom-to-tinker.com/blog/felten/drm-retreat>>. C.f. Jim Harris, “Can SanDisk prompt another digital-music revolution?” *GlobeandMail.com* (6 February 2009), online: The Globe and Mail <<http://www.theglobeandmail.com/servlet/story/RTGAM.20090206.wgtsandisk0206/BNStory/PersonalTech/home>> (reporting that SanDisk’s new music device will use DRM).

⁵¹ Peter Eckersley, “An Update on the Innards of iTunes Plus Files” EFF.org (6 June 2007), online: EFF <<http://www.eff.org/deeplinks/2007/06/update-innards-itunes-plus-files>> (reporting that individuals’ name and email address/Apples ID were accessible in files downloaded from iTunes Plus).

whether DRM ought to be used in particular ways or at all.⁵² From time to time, specific privacy-invasive practices are also brought to light, found to be illegal and redressed.⁵³ Data protection laws of general application certainly operate to regulate some activities that diminish individuals' intellectual privacy.⁵⁴ Commentary and debate over these questions continues.

Privacy regulators and policy-makers are aware of the mounting tension between copyright and intellectual privacy and have focused increased attention on the matter. For example, Canada's privacy community has voiced concern regarding DRM, particularly in the context of possible legislation that would protect the use of DRM.⁵⁵ A number of Canada's privacy commissioners

⁵² For example, independent labels reportedly urged the U.K. government to back off of providing legal protection for DRM, stating that they accept that "[t]he loss of some measure of copyright control is a factor in reaching new and enthusiastic music markets around the world." See Jonny Evans, "Indie labels reject DRM as music policeman" *Macworld* (01 February 2006), online: Macworld <<http://www.macworld.co.uk/news/index.cfm?NewsID=13739&Page=1&pagePos=2>>. A number of artists have also spoken out against DRM, including Foo Fighters, Dave Matthews Band, Switchfoot, and My Morning Jacket. See e.g. James Montgomery, "My Morning Jacket Tackle Copy-Protection Software Problems — By Burning CDs For Fans" *MTV.com* (16 December 2005), online: MTV <http://www.mtv.com/news/articles/1518240/20051215/%20my_morning_jacket.jhtml>. This dissertation does not take sides in these debates and nor need it do so. The principles and rules formulated herein are directed at the overall objectives of the legal concept of copyright as discussed in Chapter 4.

⁵³ See Part I of Chapter 3.

⁵⁴ See Part I of Chapter 5.

⁵⁵ See e.g. Canada's Privacy Community, "Letter from Privacy Community of Canada to Ministers Bernier and Oda" (17 May 2006), online: Intellectualprivacy.ca <http://www.intellectualprivacy.ca/documents/open_letter.pdf>; Canada's Privacy Community, "Background Paper: Critical Privacy Issues In Canadian Copyright Reform" (17 May 2006), online: Intellectualprivacy.ca <http://www.intellectualprivacy.ca/documents/background_paper.pdf>.

have echoed this concern.⁵⁶ The Office of the Privacy Commissioner of Canada (OPC) 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.⁵⁷

Canada's Privacy Community, "Letter from Canada's Privacy Community to Ministers Prentice and Verner" (21 January 2008), online: Intellectualprivacy.ca <http://www.intellectualprivacy.ca/wp-content/uploads/2008/01/Open_Letter-Copyright_and_Privacy-24Jan08-Final.pdf>. The author participated in drafting the 2006 letter and paper.

⁵⁶ See e.g. Letter from Jennifer Stoddart, Privacy Commissioner of Canada, to Ministers Prentice and Verner (18 January 2008), online: Office of the Privacy Commissioner of Canada (OPC) <http://www.privcom.gc.ca/parl/2008/let_080118_e.asp> [OPC, January 2008 Letter]; Letter from Jennifer Stoddart, Privacy Commissioner of Canada, to Ministers Oda and Bernier (17 May, 2006), online: OPC <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 (17 May, 2006), online: Office of the Information and Privacy Commissioner of British Columbia <http://www.oipcbc.org/publications/Comm_Public_Comments/F06-28751.pdf>; Open Letter from Ann Cavoukian, Information and Privacy Commissioner of Ontario (IPC), to Ministers Oda and Bernier (12 May, 2006), online: IPC <<http://www.ipc.on.ca/docs/drmletter.pdf>>; Letter from Frank Work, Information and Privacy Commissioner of Alberta, to Ministers Oda and Bernier (26 May, 2006), online: Office of the Privacy Commissioner of Alberta <http://www.oipc.ab.ca/ims/client/upload/Copyright_ltr_May_26_06.pdf>.

⁵⁷ See OPC, "Fact Sheet: Digital Rights Management and Technical Protection Measures" (November 2006), online: OPC <http://www.privcom.gc.ca/fs-fi/02_05_d_32_e.asp> [OPC, "DRM Fact Sheet"]. The OPC uses the term

It is likely only a matter of time before DRM or related practices are the subject of complaints under data protection laws, including Canada's data protection law, *PIPEDA*.⁵⁸

There is also a developing contemporary literature and body of law at the intersection of copyright and privacy. Leading academics, public interest groups, business leaders, policy makers, regulators, courts and others are increasingly engaged in a global dialogue regarding copyright and privacy. For example, courts and regulators are increasingly faced with cases where copyright interests are seen as pitted against privacy interests.⁵⁹ In addition, concerned about the potential consequences of yielding individuals' privacy where it conflicts with copyright holders' interests, academic commentators have conducted widespread

"TPM" in this passage. TPMs are component parts of DRM. They are described below in Chapter 3.

⁵⁸ *PIPEDA*, *supra* note 13. It must be acknowledged that such complaints would relate most closely to informational (not intellectual) privacy, though they may indirectly protect intellectual privacy in some cases. Such complaints under *PIPEDA* may also do a disservice to intellectual privacy as argued in Part I of Chapter 5.

⁵⁹ See e.g. *BMG Canada Inc v Doe*, 2005 FCA 193 [*BMG v Doe*]; *Society of Composers, Authors and Music Publishers of Canada v Canadian Assn of Internet Providers*, (2004), 240 DLR (4th) 193; (2004), 32 CPR (4th) 1, [2004] 2 SCR 427, 2004 SCC 45 [*SOCAN v CAIP*]. For examples outside Canada, see ECJ *Productores de Música de España (Promusicae) v Telefónica de España SAU*, C-275/06, [2008] ECR I-271; *Recording Indus Ass'n of Am, Inc v Verizon Internet Servs.*, 2003 US App LEXIS 25735; *Capitol Records v Does 1-16*, 2007 WL 1893603 (D New Mexico). For a discussion of some of the privacy implications of the *BMG v Doe* case, see generally Ian R Kerr & Alex Cameron, "Nymity, P2P & ISPs: Lessons from *BMG Canada Inc. v John Doe*" in Katherine J Strandburg & Daniela Stan Raicu, eds, *Privacy and Technologies of Identity: A Cross-Disciplinary Conversation* (New York: Springer, 2005) [Kerr & Cameron, "Nymity, P2P & ISPs"]; Ian Kerr & Alex Cameron, "Scoping anonymity in cases of compelled disclosure of identity: Lessons from *BMG v Doe*" in David Matheson, ed, *Contours of Privacy* (Cambridge: Cambridge Scholars Publishing, 2009).

reconnaissance for intellectual privacy; these inquiries have spanned, among other areas, freedom of expression,⁶⁰ data protection,⁶¹ human rights,⁶² and ethics.⁶³

IV. Understanding Intellectual Privacy through Books

Neither the conflict between copyright and intellectual privacy, nor the need to account for intellectual privacy within copyright, has

⁶⁰ See e.g. Cohen, "A Right to Read Anonymously", *supra* note 45 (evaluating the import of diminished intellectual privacy for traditional notions of freedom of expression and freedom of thought); Richards, *supra* note 16 (proffering that legal protection for records of intellectual activities is essential to values of free thought and expression); Ian Kerr & Jane Bailey, "The Implications of Digital Rights Management for Privacy and Freedom of Expression" (2004) 2 Info, Comm & Ethics in Society 87 at 91:

The manner in which we experience an intellectual work – in absolute solitude or under the camera's eye – must surely have an impact on our thoughts and whether we will choose to express or suppress them. DRM surveillance techniques – which have the ability to monitor what we read or listen to, when, how often, with whom we communicate about them and other related activities – are therefore inextricably tied to our ability to express ourselves freely.

⁶¹ See e.g. Greenleaf, "IP, Phone Home", *supra* note 48; Lee Bygrave & Kamiel Koelman, "Privacy, Data Protection and Copyright: Their Interaction in the Context of Electronic Copyright Management Systems" in B Hugenholtz, ed, *Copyright and Electronic Commerce: Legal Aspects of Electronic Copyright Management* (The Hague: Kluwer Law International, 2000) [Bygrave & Koelman, "Privacy, Data Protection and Copyright"]; Alex Cameron, "Digital Rights Management: Where Copyright and Privacy Collide" (2004) 2 Canadian Privacy Law Review 14 [Cameron, "DRM: Where Copyright and Privacy Collide"]; Cameron, "Learning from Data Protection Law", *supra* note 1 at 43.

⁶² See e.g. P Bernt Hugenholtz, "Caching and Copyright" (2000) 22 EIPR 482 at 485-86.

⁶³ See e.g. Ian Kerr, "Digital Locks and the Automation of Virtue" in Michael Geist, ed, *From "Radical Extremism" to "Balanced Copyright": Canadian Copyright and the Digital Agenda* (Toronto: Irwin Law, 2010) [Geist, *Balanced Copyright*].

yet attracted the attention that they merit.⁶⁴ There are a number of possible explanations for the current state of affairs. For example, the failure to delineate conditions of access to and enjoyment of copyright works, including the privacy related conditions that are the subject of this dissertation, may in part be a result of a predominant view in international copyright law over the past century that the public interest in copyright is best served by “maximum protection of creative enterprise through the grant of

⁶⁴ Indeed, Bygrave and Koelman highlight the gap in the literature in this respect as follows:

... copyright and the right to privacy can collide if they work to the advantage of opposite parties. The intersection of the right to privacy and copyright law in this regard has not yet been thoroughly researched. The issue has become of particular interest only now that new technologies – as embodied, for example, in [DRM] operations – enable the copyright-owner to monitor and control with relative ease the actual use that a person makes of a copyrighted work, thereby extending the reach of the copyright-holders

See Bygrave & Koelman, “Privacy, Data Protection and Copyright,” *supra* note 61. See also Mark Hayes, “Privacy and Copyright — An Increasingly Volatile Mixture” Blakes.com (1 August 2006), online: Blakes <http://www.blakes.com/english/view_disc.asp?ID=283> (“...courts and advocates will increasingly have to consider privacy concepts when dealing with copyright issues. What is as yet unclear is how these disparate legal concepts will be knit together into a cohesive set of principles that can be applied by copyright owners and users alike.”)

exclusive rights to authors,"⁶⁵ including through the use and legal protection of DRM.⁶⁶

It is also possible that public and policy discourse regarding copyright in the digital age has disproportionately focused on the single issue of peer-to-peer file-sharing of popular music and movies.⁶⁷ As a 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.⁶⁸ Some might conclude that activities such as

⁶⁵ P Bernt Hugenholtz & Ruth L Okediji, "Conceiving an International Instrument on Limitations and Exceptions to Copyright: Final Report" (6 March 2008) at 7, online: IVIR <<http://www.ivir.nl/publicaties/hughenoltz/finalreport2008.pdf>> [Hugenholtz & Okediji, "Conceiving an International Instrument"]. See also the abridged version of this study, published as: P Bernt Hugenholtz & Ruth L Okediji, "Contours of an International Instrument on Limitations and Exceptions" in Neil Weinstock Netanel, ed, *The Development Agenda, Global Intellectual Property and Developing Countries* (Cambridge, Oxford University Press, 2008).

⁶⁶ Another plausible contributing factor may be the tendency of legal thinkers to view privacy and freedom of expression, among other, as fundamentally constitutional rights, which are inapplicable in the private sector in general and the copyright context in particular. In addition, in liberal regimes, many people will say individuals are free to trade away whatever kinds of privacy interests they see fit to exchange for other goods, including access to materials in digital form. I am indebted to Jane Bailey for these insightful observations.

⁶⁷ See e.g. Laura J Murray, "Copyright Talk: Patterns and Pitfalls in Canadian Policy Discourses" in Geist, *In the Public Interest*, *supra* note 11 ("...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" at 27, 28).

⁶⁸ *Ibid* at 30:

... 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.

listening to ‘Top 40’ music and watching Hollywood movies, for example, like walking through parking lots, do not attract a strong expectation of intellectual privacy.⁶⁹ For some, these categories of creative works might not *prima facie* implicate deeply-held principles regarding the importance of intellectual privacy in the same way that political or religious writings might.

As more and more forms of copyright works are digitized and more and more forms of information created and disseminated exclusively 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 and are available for free download from at least two different sources on the Internet.⁷⁰ 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

⁶⁹ See Chapter 2 and Part I of Chapter 5. The use of the words “parking lots” is an allusion to a landmark decision under *PIPEDA* discussed in Chapter 5: OPC, “*PIPEDA* Case Summary #114: Employee Objects to Company’s Use of Digital Video Surveillance Cameras” (6 November, 2003), online: OPC <http://www.privcom.gc.ca/cf-dc/2003/cf-dc_030123_e.asp>; *Eastmond v Canadian Pacific Railway* (2004), 16 Admin LR (4th) 275 (FCA) [*Eastmond*].

⁷⁰ Each of these works has 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=FKINmiM4GJwC&pg=PA1&dq=rights+of+man>>, *The Clockmaker* Project Gutenberg edition <<http://www.gutenberg.org/dirs/etext04/clckm10.txt>>, Google Books edition <http://books.google.com/books?id=8o4lAAAAMAAJ&pg=PA1&dq=the+clock+maker&as_brr=1>.

texts searchable, in the same way that Web sites can be searched on the company's engine at google.com."⁷¹ Numerous libraries and archives around the world are engaged in similar projects, as are publishers and book distributors.⁷² Audio books are widely available online.⁷³ A staggering volume of literary works are now available online and in electronic form. In 2010, Amazon.com

⁷¹ Jeffrey Toobin, "Google's Moon Shot: The quest for the universal library" *The New Yorker* (5 February 2007) 30 at 30.

⁷² See e.g. James Adams, "Indigo launches e-book service" *Globe and Mail* (25 February 2009) R1; Hathi Trust, "Welcome to the Shared Digital Future: HathiTrust Launched," online: Hathi Trust, <<http://www.hathitrust.org/>> (this is a digital repository of a number of major American research libraries with over 2.2 million volumes digitized as of October 2008); University of Michigan Library, "One Million Digitized Books" (2 February 2008), online: University of Michigan <<http://www.lib.umich.edu/news/millionth.html>> (in partnership with Google); Cristina Jimenez, "British Library books go digital" *BBC News* (28 September 2007), online: BBC <<http://news.bbc.co.uk/2/hi/technology/7018210.stm>>; Kate Hafner, Libraries Shun Deals to Place Books on Web, *New York Times* (22 October 2007), online: New York Times <http://www.nytimes.com/2007/10/22/technology/22library.html?_r=1&emc=eta1&oref=slogin>; Doreen Carvajal, "U.S. Library of Congress introduces plans for world digital collection" *International Herald Tribune* (17 October 2007), online: International Herald Tribune <<http://www.iht.com/bin/printfriendly.php?id=7932556>>. The example of eReader was discussed above in this chapter. See also Reuters, "Report: Random House to sell book chapters" (11 February 2008), online: News.com <http://www.news.com/2110-1026_3-6229985.html>; Sturgis Library, "Barnstable Patriot", online: Sturgis Library <<http://www.sturgislibrary.org/collections/barnstable-patriot>> (digital archive of the Barnstable Patriot, the seventh oldest newspaper in the United States); Associated Press, "Random House to digitize thousands of books" *washingtonpost.com* (24 November 2008), online: Washington Post <<http://www.washingtonpost.com/wp-dyn/content/article/2008/11/24/AR2008112400652.html>>.

⁷³ See e.g. Librivox, "Librivox: acoustical liberation of books in the public domain", online: Librivox <<http://librivox.org/>>.

reported that sales of electronic books for its Kindle device had surpassed sales of hardcover books.⁷⁴

Using digitization to increase access to the information contained in books is certainly laudable, providing an unprecedented, convenient, cost-effective and powerful means to search for, access and use the information contained in books. However, digitizing books does not come without risk.⁷⁵ If DRM or other means of diminishing privacy were used in association with “every book ever published,” the traditional relationship between copyright and

⁷⁴ Adam Ostrow, “Amazon: Kindle Books Now Outselling Hardcovers” *Mashable* (19 July 2010), online: Mashable <<http://mashable.com/2010/07/19/amazon-kindle-sales/>>.

⁷⁵ See e.g. Nick Collins, “E-books threaten livelihoods of aspiring writers” *The Telegraph* (18 August 2011), online: The Telegraph <<http://www.telegraph.co.uk/technology/news/8706797/E-books-threaten-livelihoods-of-aspiring-writers.html>>; Robert Darnton, “The Library in the New Age” *New York Review of Books* (12 June 2008), online: New York Review of Books <<http://www.nybooks.com/articles/21514>> (arguing that Google Book Search suffers from a number of shortcomings and that it makes research libraries more important than ever). Insofar as search engines are concerned, as discussed in Chapter 3, there are reasons to be concerned about intellectual privacy in connection with the Google's activities, including Google Book Search. See e.g. Privacy International, “A Race to the Bottom - Privacy Ranking of Internet Service Companies” (6 September 2007), online: Privacy International <<http://www.privacyinternational.org/article.shtml?cmd%5B347%5D=x-347-553961>> (ranking Google at the bottom of its privacy ranking in the category “[c]omprehensive consumer surveillance & entrenched hostility to privacy”). For a general discussion of the privacy issues that search engines can raise, see Article 29 Data Protection Working Party, “Opinion on data protection issues related to search engines” /08/EN/WP (04 April 2008); International Working Group on Data Protection in Telecommunications, “International Documents on Data Protection in Telecommunications and Media 1983 – 2006”, online: Datenschutz <http://www.datenschutz-berlin.de/attachments/334/IWGDPT_WP_brochure.pdf> (“search engines have the capability to draw up a detailed profile of the interests of their users” at 63).

intellectual privacy would be rewritten; it would be written into the terms of the DRM-enabled licenses or privacy policies of the copyright holder or other entity that delivered books to individuals.⁷⁶

Google Books, for example, utilizes a form of DRM to restrict certain activities, including individuals' ability to print or otherwise save copies of pages or whole books offered through the service in some cases. Like eReader, Google Books permits individuals to select portions of books and to save or share them in certain ways. For example, individuals can highlight sections of *Rights of Man* and *The Clockmaker* to save to Google Notebook as images, or copy portions of text when viewing the books as plain text. These books can also be downloaded to an individual's computer or added to Google's My Library feature.

Individuals' use of Google Books to access *Rights of Man*, *The Clockmaker* and other books available through the service is subject to Google's Privacy Policy which explains how Google collects, uses and discloses information about individuals.⁷⁷ A core element of Google's business model is online advertising based on information about individuals' online activities, including the use of Google Books.⁷⁸ Access to *Rights of Man* on Google Books, for example, is accompanied by links to purchase the book from a

⁷⁶ See Toobin, *supra* note 71.

⁷⁷ Google's privacy policy is found at the following link: <<http://books.google.ca/intl/en/privacypolicy.html>>

⁷⁸ See generally Chris Castle, "Is Google's culture grab unstoppable? Monopoly Money from Digital Books" *The Register* (31 December 2008), online: The Register <http://www.theregister.co.uk/2008/12/31/chris_castle_google_books_and_beyond/>. See also Russ Mitchell, "Search Mission" *Conde Naste Portfolio.com* (April 2008), online: Portfolio.com <<http://www.portfolio.com/executives/features/2008/03/14/Google-CEO-Eric-Schmidt-Interview>> (interview with Google CEO Eric Schmidt discussing Google's internet-search-driven advertising business model).

variety of retailers, and by “Sponsored Links” which advertise “Us Citizen Rights: Find more sources/options for Us Citizen Rights, www.webcrawler.com.”⁷⁹

Although there are potentially a number of ways that Google’s Privacy Policy may affect intellectual privacy,⁸⁰ including in connection with online advertising, it is worth noting two obvious elements of the Google Books service that implicate intellectual privacy. First, some information is clearly made public: “When you add reviews, ratings, notes, or labels to a book—or when you add a book to your my Library page—that information will be publicly displayed on Google Book Search.”⁸¹ Second, Google openly acknowledges that it tracks some of the books and pages that individuals access in certain circumstances:

In order to protect copyrighted books, we only allow Google Book Search users to view a limited portion of the book we present. Enforcing these limits requires us to keep track of our users' page views. [...] Once you log in, [...] to enforce limits on user page views, we do connect some information -- your Google Account name -- with the books and pages that you've viewed. As always, we strongly encourage you to read our

⁷⁹ Thomas Paine, *Rights of Man, Common Sense, and Other Political Writings* (Oxford: Oxford University Press, 1995), online: Google <<http://books.google.com/books?id=FGquAAAACAAJ&dq=rights+of+man&ei=WKKJSYeXJ6OSkATb6YmNAg>>. The quoted advertisement is one that appeared when the author viewed the book. However, Sponsored Links will potentially change over time as different organizations advertise through Google.

⁸⁰ For example, see the concerns reflected in Privacy International, *supra* note 75.

⁸¹ Google, “Who will see my book reviews, library and annotations?”, online: Book Search Help Center <<http://books.google.com/support/bin/answer.py?answer=100088>>.

Privacy Policy to be fully informed about how your confidentiality is protected.⁸²

Although it was ultimately rejected by the court in 2011, Google's proposed settlement with the Authors Guild, the Association of American Publishers and other authors and publishers in connection with its Google Books project included a number of measures which would have implicated intellectual privacy. Google intended to use technological measures to place a watermark on printed pages with encrypted information that identifies the individual that printed the copy of the book page, including in situations where an individual accesses a book through Google Books at their library.⁸³ A number of groups opposed the proposed settlement on the basis of privacy. The court noted these objections in the decision rejecting the proposed settlement, as follows:

Certain objectors, including the Center for Democracy and Technology and the Electronic Privacy Information Center, contend that the [Amended Settlement Agreement or ASA] raises significant privacy issues, as the digitization of books would enable Google to amass a huge collection of information, including private information about identifiable users, without providing adequate protections regarding the use of such information. [...]

⁸² Google, "Google Book Search Common Questions", online: <<http://books.google.com/googlebooks/common.html#11>>. Google's landmark proposed settlement of a class action lawsuit brought by authors and publishers provides further insight into the ways that individuals' personal information may be implicated in Google Books in future. The proposed settlement is discussed below and in Chapter 3.

⁸³ See Google, "Google Book Search Copyright Settlement", online: <<http://books.google.com/booksholders/agreement-contents.html>> at pages 47 – 48 of the Settlement Agreement [Google Settlement Agreement]. See also *Authors Guild v Google Inc.*, 05 Civ. 8136 (Opinion, March 22, 2011) (rejecting the proposed settlement).

The Consumer Watchdog, Privacy Authors and Publishers, and others raise privacy concerns. The Consumer Watchdog argues that the ASA would give Google "the ability to collect nearly unlimited data about the activities of users of its Book Search and other programs, including users' search queries, the identity of books a particular user reads, how long that reader spends on each book, and even what particular pages were read." These objectors contend that the ASA fails to provide adequate protections for users of Google Book Search. They contend that the ASA fails to follow established law that protects reader privacy by limiting the disclosure of reader information.

The privacy concerns are real. Yet, I do not believe that they are a basis in themselves to reject the proposed settlement. The ASA provides that contact information provided by Class members to the Registry will not be disclosed to Google or the public if the Class member so requests. (ASA§ 6.6(c)(iii), (d)). It also provides that Google shall maintain in confidence any Rightsholder's personally identifiable information received in connection with the settlement. (ASA § 6.6(f)). Google has "committed" to certain safeguards, although these are voluntary undertakings only. I would think that certain additional privacy protections could be incorporated, while still accommodating Google's marketing efforts.⁸⁴

As the examples of Google Books and eReader illustrate, the conditions of intellectual privacy originally associated with access to *Rights of Man* and *The Clockmaker* have changed dramatically in the digital age.

It is in access to books, newspapers, magazines, journal articles, and other literary works that questions of intellectual exploration,

⁸⁴ *Authors Guild v Google Inc*, *ibid* [citations and references omitted].

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 more patently pressing in light of the potential for the increased digitization of literary works. Although principles and rules that account for intellectual privacy in copyright must account for modern and future forms of creative works, the digitization of books is offered as an example in this chapter because it provides an easy insight into the reasons why questions at the nexus of copyright and intellectual privacy are important. However, it is important to reiterate that although books offer easy insight into questions of intellectual privacy, this dissertation resists the notion that distinctions between various forms of copyright works ought to dictate whether or how much intellectual privacy individuals should be entitled to in their access to and enjoyment of works.⁸⁵

V. Overview of Contents

Predicting the future state of copyright, technology, the market or intellectual privacy is not the object of this dissertation. We may end up in a world where we 'tap into the beam'⁸⁶ and have digital access to every book ever published; then again, we may not.⁸⁷ The perspective taken here is that, irrespective of what the future may

⁸⁵ See Part I(B) of Chapter 5.

⁸⁶ David Gelernter, "Tapping into the Beam" in John Brockman, ed, *The Next Fifty Years: Science in the First Half of the Twenty-First Century* (New York: Vintage Books, 2002) (offering a prediction of the state of computer technology in or about the year 2050).

⁸⁷ Of course, it seems likely that no matter what the future holds, we will continue to read tangible, physical copies of books even if digital books may take on an increasing share of the book market. See generally Library Journal, "At Frankfurt, Many Say Digital Will Take Over Print Books by 2018" *LJ Academic Newswire* (21 October 2008), online: Library Journal <<http://www.libraryjournal.com/eNewsletter/CA6607393/2673.html>>.

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 role of intellectual privacy *within* the legal concept of copyright.

This dissertation does not assert that we ought to privilege intellectual privacy issues over the myriad other privacy issues present in the digital age. Instead, by accounting for intellectual privacy within copyright, this dissertation resolves conflict between copyright and intellectual privacy in ways that are primarily relevant to copyright objectives but which in no way purports to advantage them over situations of conflict between privacy and other interests and rights. Indeed, while changes to privacy legislation and other regulatory instruments may assist in addressing intellectual privacy challenges and other privacy issues in the digital age, it is suggested here that intellectual privacy requires specialized consideration and that copyright law is an important place to develop rules for its protection.

Chapter 2 articulates a definition of intellectual privacy as distinct from other forms of privacy and underscores the important values that are related to this concept. The definition of intellectual privacy described in Chapter 2 is largely developed in reference to individuals' interactions with copyright works and the acts of reading, writing and thought. In developing the definition, Chapter 2 provides a basic introduction to legal concepts of privacy, including the values that are interrelated with privacy and closely related concepts such as freedom of expression.

Chapter 3 maps contemporary conflict between copyright and intellectual privacy. This chapter describes the technologies, laws and intermediaries at play at the intersection of copyright and intellectual privacy, including specific examples of conflict that have arisen to date in the digital era. Although Chapter 3 is primarily descriptive, the examples described therein are

illustrative of the deeper relationship between copyright and intellectual privacy, as well as a broad view of what might count as an invasion of intellectual privacy in connection with creative works.

Chapter 4 shifts our attention to the world of copyright law. This chapter begins with a basic introduction to copyright, including literature on the objectives of copyright law in Canada.⁸⁸ In search of support for the notion that copyright ought to provide a fuller account of intellectual privacy, Chapter 4 provides an account of the traditional relationship between copyright and intellectual privacy. At first blush, one might have thought that copyright and intellectual privacy have come to implicate one another only over the course of the past decade since the advent of digital networked technology. The kinds of conflicts that have emerged in the recent past as described in Chapter 3 do appear to be a uniquely contemporary phenomenon. However, copyright and intellectual privacy also share a much older and more foundational relationship. Chapter 4 exposes a variety of ways that copyright already recognizes the values of intellectual privacy, including authors' right of first publication and moral rights. Building on these principles, this chapter argues that intellectual privacy is an essential component of copyright as a unified whole and that copyright must account for intellectual privacy as proposed in Chapter 5.

⁸⁸ The purposes of Canadian copyright law are a matter of some uncertainty and debate. See generally Teresa Scassa, "Interests in the Balance" in Geist, *In the Public Interest*, *supra* note 11 [Scassa, "Interests in the Balance"]. This dissertation does not purport to define the purposes of copyright law in Canada. Instead, this dissertation explores how intellectual privacy might be accounted for in competing understandings of the purposes of copyright in Canada. See also, Teresa Scassa, "Overbalancing: The Supreme Court of Canada and the Purpose of Canada's Copyright Act" (2009) 25 CIPR 181 [Scassa, "Overbalancing"].

Finally, Chapter 5 explores what a copyright law that accounts for intellectual privacy might look like. With reference to the copyright principles discussed in Chapter 4, this chapter addresses the ‘how’ of copyright and intellectual privacy – it explores potential solutions (and elements thereof) and makes five basic recommendations for rules to account for intellectual privacy within copyright. Intellectual privacy is advanced as an important condition that should be present in individuals’ access to copyright works. Chapter 5 does not assert that the copyright solutions proposed are a sufficient solution for the challenges to intellectual privacy described herein. While the solutions proposed will cover a lot of creative works for a significant period of time (during which the works are protected by copyright), it must be acknowledged that intellectual privacy in relation to non-copyright works and works in which copyright has expired will not be addressed directly by the solutions proposed in Chapter 5. Other solutions and future work in the area will need to be explored. With the framework proposed, it is hoped that conflict between copyright and intellectual privacy will be avoided in future, without the need to specifically predict what the future will be.

CHAPTER 2:

INTELLECTUAL PRIVACY

I. Introduction

In 1836, Charles Darwin returned to England from his historic voyage aboard H.M.S. *Beagle*. On September 14, 1842, he and his family moved to Down House, a rural home in London Borough of Bromley.⁸⁹ It was at this house that Darwin developed his ideas on evolution and wrote one of the most revolutionary scientific works of all time, *On the Origin of Species*, first published in 1859.⁹⁰

While at Down House, Darwin built an important addition to the property that would come to play a central role in his intellectual

⁸⁹ Darwin lived in Down House until his death in 1882. He died at the house. See generally Charles Darwin, (Nora Barlow, ed), *The Autobiography of Charles Darwin 1809–1882* (London: Collins, 1958) at 114; English Heritage, “The Home of Charles Darwin, Down House Background Information”, online: English Heritage <<http://www.english-heritage.org.uk/server/show/nav.14927>>.

⁹⁰ Charles Darwin, *On the Origin of Species By Means of Natural Selection* (London: John Murray, 1859). The first edition of *On the Origin of Species* is available in electronic format for download from a variety of sources on the Internet, including from Project Gutenberg at <<http://www.gutenberg.org/etext/1228>>.

endeavours: his now-famous Sandwalk.⁹¹ Still present at Down House today, the Sandwalk is a sand-covered path that “winds through the shady woods and then returns toward the house along a sunny, hedge-lined field.”⁹² Darwin walked the Sandwalk each day. He referred to it as his “thinking path”:

Often [Darwin] would stack a few stones at the path’s entrance, and knock one away with his walking stick on completing each circuit. He could anticipate a ‘three-flint problem,’ just as Sherlock Holmes had ‘three-pipe problems’, and then head home when all the stones were gone.⁹³

Darwin’s ability to retreat to the solitude of the Sandwalk played an essential role in the development and expression of his ideas. Similarly, his famous expeditions in South America gave him “the

⁹¹ Richard Milner, “Keeping Up Down House” (1996) 105 *Natural History* 54-57. See also Francis Darwin, *The Life and Letters of Charles Darwin: Including an Autobiographical Chapter* (London: John Murray, 1888) at 93-94. Given the subject matter of this dissertation, one might think it an unfortunate coincidence that Darwin’s Sandwalk was in fact located on property that Darwin rented on an annual basis from his neighbour and friend, Sir John Lubbock (Lord Avebury). See E Janet Browne, *Charles Darwin: The Power of Place* (Princeton: Princeton University Press, 2002) at 402. However, just the opposite may be true. Without suggesting that access to copyright works is or should be analogous to a tenancy (which may be a matter for another author to explore), it is important to note that tenants have a common law right to quiet enjoyment of property: the covenant of quiet enjoyment “promis(es) that the tenant... shall enjoy the possession and use of the premises in peace and without disturbance. In connection with the landlord-tenant relationship, the covenant of quiet enjoyment protects the tenant’s right to freedom from serious interferences with his or her tenancy.” See *Black’s Law Dictionary*, 6th ed, *sub verbo* “covenant of quiet enjoyment”.

⁹² Milner, *ibid*.

⁹³ *Ibid*. See also, Darwin, *supra* note 89 at 93; Adrian J Desmond & James Moore, *Darwin: The Life of a Tormented Evolutionist* (New York: W W Norton & Company, 1994) at 336.

leisure and the intellectual privacy to contemplate freely and at length"⁹⁴:

...by getting away from Cambridge and England he was escaping from a mental climate in which certain thoughts were unthinkable. On the other side of the world, especially during the lengthy periods spent exploring the South American continent, well removed from the company of the *Beagle's* ultra-conservative captain, Robert Fitzroy, there was little to constrain Darwin's thinking.⁹⁵

Darwin's "thinking path" and overseas adventures, each far from the crowds of "vile smoky"⁹⁶ London, are emblematic of aspects of the relationship between privacy and the exploration, development and expression of ideas. Although ideas and expression can find their genesis in a wide variety of circumstances, including on a crowded streetcar or in collaborative or group environments,⁹⁷

⁹⁴ *Ibid* at 52.

⁹⁵ *Ibid.* See also Michael JA Howe, *Genius Explained* (Cambridge: Cambridge University Press, 1999) (discussion the ways that great thinkers have achieved the necessary private space and "a degree of separation from the pressures of other people and their demands" at 55).

⁹⁶ Charles Darwin, Letter to Leonard Jenyns (10 April 1837), online: Darwin Correspondence Project <<http://www.darwinproject.ac.uk/darwinletters/calendar/entry-354.html>>. In this letter, Darwin also stated "I do hate the streets of London."

⁹⁷ For example, Darwin often had visitors at Down House and exchanged correspondence about his ideas with his colleagues. See Karin Schutjer, "Aground of One's Own: Hölderlin, *Eigentum* and *Eigentümlichkeit*" in Martha B Helfer, ed, *Rereading Romanticism* (Amsterdam: Rodopi, 2000) (characterizing the German poet Hölderlin's time as a family tutor in 1794 as offering him "both social exchange and intellectual privacy" at 170); William Howard Adams, *The Paris Years of Thomas Jefferson* (Yale: Yale University Press, 2000) at 109. See also Ronda Kaysen, "Stop Thinking and Have an Idea-The Casual Way to Get Creative" *New York Observer* (9 November 2003), online: Observer.com <<http://www.observer.com/node/48309>> ("Space, privacy and quiet time are not necessarily conducive to creativity").

individuals often require intellectual privacy—a “breathing space” removed from others⁹⁸—in order to freely explore, develop and express their thoughts. Yet, this assertion should not be read as detracting from the argument, also supported in this dissertation,⁹⁹ that authorship and creativity depend to a very large degree on social interaction¹⁰⁰ and on access to the ideas and expressions of others.¹⁰¹ Notwithstanding the “great author”¹⁰² phenomenon of the nineteenth century, which persists in contemporary copyright,¹⁰³ it has long been observed that individuals’ ideas build and reflect on the ideas of others that have come before. Although Isaac Newton is oft-quoted for stating “[i]f I have seen a little further, it is by standing on the shoulders of Giants”, the phrase was originally uttered by Bernard of Chartres in the twelfth century:

⁹⁸ Cohen, “DRM and Privacy”, *supra* note 3 (“Properly understood, an individual’s interest in intellectual privacy has both spatial and informational aspects. At its core, this interest concerns the extent of ‘breathing space,’ both metaphorical and physical, available for intellectual activity” at 576). See also Peter K Yu, *Intellectual Property and Information Wealth: Issues and Practices in the Digital Age* (Westport: Greenwood, 2007) [Yu, *Intellectual Property and Information Wealth*] (“Intellectual privacy refers to the right to experience intellectual works in private, free from surveillance.” at 338); Richards, *supra* note 16 (“Intellectual privacy is the ability, whether protected by law or social circumstances, to develop ideas and beliefs away from the unwanted gaze or interference of others” at 389). These and other definitions of intellectual privacy are considered below in Part III of this chapter.

⁹⁹ See Chapters 2 and 4.

¹⁰⁰ See generally *supra* note 95 and accompanying text.

¹⁰¹ I am grateful to Jane Bailey for this important point and for the suggestion that it be mentioned here.

¹⁰² See generally Carys Craig, “Reconstructing the Author-Self: Some Feminist Lessons for Copyright Law” (2007) 15 *Journal of Gender, Social Policy & the Law* 207 at 213 [Craig, “Reconstructing the Author-Self”] citing and quoting, *inter alia*, Marilyn Randall, *Pragmatic Plagiarism: Authorship, Profit and Power* (Toronto: University of Toronto Press, 2001).

¹⁰³ *Ibid.*

Bernard of Chartres used to say that we [the Moderns] are like dwarves perched on the shoulders of giants [the Ancients], and thus we are able to see more and farther than the latter. And this is not at all because of the acuteness of our sight or the stature of our body, but because we are carried aloft and elevated by the magnitude of the giants.¹⁰⁴

More recently, Craig has asserted that we can “re-imagine the author not as source, origin, or authority, but as participant, citizen,”¹⁰⁵ thus highlighting:

the nature of authorship as a social and formative process [and offering] the foundation for a coherent justification of copyright: copyright law, which aims to encourage creativity and exchange, should thereby encourage participation in cultural dialogue and facilitate the relations of communication that are central to this conception of selfhood and society.¹⁰⁶

The concept of intellectual privacy advanced in this dissertation is compatible with concepts of aloneness and “breathing space” and with relational aspects of authorship and creation – e.g. social interaction and “standing on the shoulders of giants.” Indeed, a core element of the objectives of this dissertation is to demonstrate that intellectual privacy is an important condition under which individuals must be able to search for, access, enjoy and build on the works of others.

Building on the basic observations expressed above, this chapter seeks to articulate a definition of intellectual privacy as distinct

¹⁰⁴ See Scott D Troyan, *Medieval Rhetoric: A Casebook* (London: Routledge, 2004) at 10. In more recent times, Ella Fitzgerald famously stated: “I stole everything I ever heard, but mostly I stole from the horns.”

¹⁰⁵ Craig, “Reconstructing the Author-Self”, *supra* note 102 at abstract.

¹⁰⁶ *Ibid.*

from other forms of privacy. For example, as Darwin's experience suggests, intellectual privacy can often be achieved in whole or in part through different forms of spatial privacy. Yet, this chapter asserts that intellectual privacy is also distinct from spatial privacy (and other forms of privacy) and that it is related to a distinct set of values. The strong links between intellectual privacy and values of free thought, expression, creative endeavour, identity, autonomy and personal development.¹⁰⁷ are of particular significance in light of the ultimate objective of this dissertation: to explore whether and how copyright should account for intellectual privacy. Thus, in describing what intellectual privacy is, this chapter places special emphasis on individuals' interactions with copyright works.¹⁰⁸

¹⁰⁷ Remaining with Darwin for a moment, one Darwin scholar notes that:

[f]ive years on board the *Beagle* taught Darwin to think for himself and allowed him... to envision himself as a theoretician with a penchant for far-reaching explanations and universal laws. Once the anxious collector on the *Beagle* was transformed into an increasingly bold geological theorist, Darwin was able to transfer his developing intellectual talents to many other fields of science. [...] In the process, the voyage provided Darwin with something much more important, namely the opportunity to mature intellectually under highly auspicious circumstances and thereby to become the Darwin that history now celebrates. [...] ...Darwin's personal transformation in self-confidence and self-identity – not any specific scientific discovery of his famous Galapagos visit – was actually the *Beagle* voyage's most important contribution to his subsequent success in science.

See Frank J Sulloway, "Darwin's Early Intellectual Development: An Overview of the *Beagle* Voyage" in David Kohn, ed, *The Darwinian Heritage* (Princeton: Princeton University Press in association with Nova Pacifica, 1985) at 146-47.

¹⁰⁸ Such interactions are an area where intellectual privacy has traditionally been recognized and valued. See the discussion in Part IV of Chapter 1, which places a particular emphasis on interactions with books. See also The American Library Association, "Privacy: An Interpretation of the Library Bill of Rights", (2002) [ALA, "Interpretation of the Library Bill of Rights"]:

The above said, this chapter does not argue that intellectual privacy is or should be limited only to the conditions under which individuals access and enjoy copyright works. Indeed, Darwin enjoyed a form of intellectual privacy while walking on his Sandwalk but he was not accessing any copyright works at the time; he might have been liable to trip over his own walking stick. Nor does copyright cover all forms of “creations of the mind”¹⁰⁹ or myriad other activities to which a robust concept of intellectual privacy should *prima facie* attach.¹¹⁰

In all areas of librarianship, best practice leaves the user in control of as many choices as possible. These include decisions about the selection of, access to, and use of information. Lack of privacy and confidentiality has a chilling effect on users’ choices. All users have a right to be free from any unreasonable intrusion into or surveillance of their lawful library use.

The emphasis on copyright works in this chapter is also relevant because intellectual privacy is strained by copyright in the digital age as described in Chapters 1 and 3.

¹⁰⁹ See World Intellectual Property Organization, “What is Intellectual Property?”, online: WIPO <<http://www.wipo.int/about-ip/en/>>:

Intellectual property refers to creations of the mind: inventions, literary and artistic works, and symbols, names, images, and designs used in commerce. [...] Intellectual property is divided into two categories: Industrial property, which includes inventions (patents), trademarks, industrial designs, and geographic indications of source; and Copyright, which includes literary and artistic works such as novels, poems and plays, films, musical works, artistic works such as drawings, paintings, photographs and sculptures, and architectural designs.

The values related to intellectual privacy may also require that individuals have intellectual privacy in respect of any number of factual or other sources of information that may not be protected by copyright or other intellectual property laws. For a discussion of fact-based works, see Teresa Scassa, “Copyright Reform and Fact-Based Works” in Geist, *Balanced Copyright*, *supra* note 63.

¹¹⁰ For example, the act of communication may implicate intellectual privacy in many cases, whether or not it relates in any way to copyright works. See

In addition, this chapter does not assert that intellectual privacy is worthy of protection only for the likes of Darwin. To the contrary, this chapter argues that intellectual privacy is crucial for and is related to values that are essential for people from all walks of life, including creators and those who seek to access and enjoy creative works and other information. For example, intellectual privacy is important for individuals seeking information about *inter alia* political views, a suspected health condition, or escaping an abusive relationship. Conditions of intellectual privacy in these and other contexts are important not (only) because of a connection with the relational aspects of creative endeavour¹¹¹ but because values such as freedom of thought, autonomy, identity and expression (and in some cases personal safety) demand such conditions. In other words, while one of the values of intellectual privacy lies in its relationship with creative endeavour, there are a variety of other values that are related to intellectual privacy that have little or nothing to do with creative endeavour *per se*. Such values are explored in Part III of this chapter.

Accordingly, although the focus of this dissertation is on copyright and creative endeavor, and on the relationship between those concepts and intellectual privacy, this chapter contains reminders that intellectual privacy matters for much more than copyright and to many more people than just authors and prospective authors of copyright works. Indeed, at a fundamental level, intellectual privacy helps ensure that individuals have the ability to access an adequate range of life's options, thereby fostering *self-creation* and *moral authorship*. Discussing the various restrictions that can be imposed by DRM systems and legal protections for such systems,

generally Richards, *supra* note 16. But see Marc Jonathan Blitz, "The Where and Why of Intellectual Privacy" (2009) Tex L Rev 15 at 19-20 (noting that intellectual privacy cannot shield every activity); Christopher Slobogin, "The Meaning of "Intellectual Privacy" (2009) 87 Tex L Rev 25.

¹¹¹ See *supra* note 106 and accompanying text.

which can include restrictions that diminish intellectual privacy as discussed herein, Kerr posits that:

[i]f we are to remain, to a considerable degree, the authors of our moral world, we must maintain the ability to access it and make use of it. While the law of copyright affords protection to the creators of original works, a balanced copyright scheme must not, in the process, diminish the very possibility of self-creation. Excessive protection of digital locks places coercive limits on moral actors, preventing them from acquiring access to an adequate range of life's options. What would be the point in developing entire systems to protect creative works or other forms of property if the means by which this is achieved ultimately undermines moral authorship and the project of conscious self-creation?¹¹²

¹¹² Ian Kerr, "Digital Locks and the Automation of Virtue" in Geist, *Balanced*, *supra* note 109 at 303. In support of this passage, Kerr quotes from the philosopher Joseph Raz on the relationship between the morality of freedom and copyright law's concept of authorship. See Joseph Raz, *The Morality of Freedom* (New York: Oxford University Press, 1986) at 86, 390:

All too often moralists tend to regard a person's moral life as the story of how he proves himself in the face of moral demands imposed on him by chance and circumstance. Crucial as this aspect is, it is but one side of a person's moral history. The other side of the story evolves around the person not as the object of demands imposed from the outside, but as the creator of such demands addressed to himself. We are all to a considerable degree the authors of our moral world. [...] Autonomy requires that self-creation must proceed, in part, through choice among an adequate range of options; that the agent must be aware of his options and of the meaning of his choices; and that he must be independent of coercion and manipulation by others. Personal autonomy is the ideal of free and conscious self-creation.

Part II of this chapter highlights a number of key legal protections for privacy in Canada.¹¹³ This overview provides an important context for the definition of intellectual privacy described in Part III and introduces concepts that may inform the component parts of the solutions described in Chapter 5. Part III of this chapter sets forth a definition of intellectual privacy, including a description of some of the values which are related to this concept. Finally, Part IV explores some of the important limits of the definition of intellectual privacy proffered herein.

II. Privacy

The poorest man may in his cottage bid defiance to all the forces of the Crown. It may be frail — its roof may shake — the wind may blow through it — the storm may enter — the rain may enter — but the King of England cannot enter! — all his force dares not cross the threshold of the ruined tenement.

- William Pitt, 1763¹¹⁴

Privacy has famously been characterized as the “right to be let alone”¹¹⁵. Yet, despite the elegant simplicity of that definition, nearly every author to write about privacy acknowledges that

¹¹³ This chapter does not provide an exhaustive review of the myriad privacy protections in Canada. For further reading, see generally Barbara McIsaac, Rick Shields & Kris Klein, *The Law of Privacy in Canada* looseleaf (Toronto: Carswell, 2000).

¹¹⁴ Lord H Brougham, *Historical Sketches of Statesmen Who Flourished in the Time of George III* (1855), vol I, at 42, quoting William Pitt, Speech on the Excise Bill, House of Commons (March 1763). See also *Semayne’s Case*, [1558-1774] All ER Rep 62 (1604 (“... the house of everyone is to him as his castle and fortress/ as well for his defence against injury and violence, as for his repose” at 63); *Eccles v Bourque*, (1975) 2 SCR 739 at 742-43.

¹¹⁵ SD Warren & LD Brandeis, “The Right to Privacy” (1890) 4 Harv L Rev 193 at 193.

privacy has not been and likely cannot be clearly defined.¹¹⁶ Privacy appears to have as many different meanings as there are authors, people and fact situations in our world;¹¹⁷ indeed, "...the constitutive elements in the veritable plethora of tangible and intangible interests that together form our varying conceptions of privacy are exceedingly difficult to define."¹¹⁸ Solove has recently asserted that privacy "is a concept in disarray" and that "[n]obody can articulate what it means."¹¹⁹ In addition, some emerging literature emphasizes that privacy is more than an individual right because "it serves other important [social] functions beyond those

¹¹⁶ See generally Judith Jarvis Thomson, "The Right to Privacy" (1975) 4 *Philosophy and Public Affairs* 295 ("Perhaps the most striking thing about the right to privacy is that nobody seems to have any very clear idea what it is" at 295); Richard A Posner, "The Right of Privacy" (1978) 12 *Ga L Rev* 393 ("The concept of 'privacy' is elusive and ill defined. Much ink has been spilled in trying to clarify its meaning" at 393); David Brin, *The Transparent Society: Will Technology Force Us to Choose Between Privacy and Freedom?* (Reading: Addison Wesley, 1998) ("From philosophers to steelworkers, it seems that each person views such things differently. Especially privacy, which, like the fabled elephant fondled by a dozen blind sages, is described uniquely by each beholder" at 14); Priscilla M Regan, *Legislating Privacy: Technology, Social Values, and Public Policy* (Chapel Hill: University of North Carolina Press, 1995) (reviewing a number of writings and emphasizing that privacy has been difficult to define, at 3); Dean Prosser, "Privacy" (1960) 48 *Cal L Rev* 383 at 389 (privacy as four distinct torts); Allen Linden, *Canadian Tort Law*, 7th ed (Markham: Butterworths, 2001) at 56-60 (noting that Canadian courts have thus far clearly recognized only the fourth of Prosser's privacy torts – misappropriation of personality); Edward Bloustein, "Privacy as an Aspect of Human Dignity", (1964) 39 *NYUL Rev* 962 at 971 (conceptualizing privacy is an interest of the human personality which protects independence, dignity and integrity).

¹¹⁷ For a general discussion of the background, history, and value of privacy, see Kevin M Keenan, *Invasion of Privacy: A Reference Handbook* (Santa Barbara: ABC-CLIO, 2005). See also *ibid*.

¹¹⁸ Ian R Kerr & Jena McGill, "Emanations, Snoop Dogs and Reasonable Expectation of Privacy" (2007) 52 *Crim LQ* 392 at 417.

¹¹⁹ Daniel J Solove, *Understanding Privacy* (Cambridge: Harvard University Press, 2008) at 1.

to the particular individual”¹²⁰ and should be understood as a social value and construction.¹²¹

Notwithstanding the apparent lack of clarity about the meaning(s) of privacy, there is little doubt that the protection of privacy is recognized around the world as a matter of utmost importance, a fundamental human right,¹²² particularly in our information age.¹²³ Said to be “the most comprehensive of rights and the right most

¹²⁰ Regan, *supra* note 116 at 16.

¹²¹ See e.g. Valerie Steeves, “Reclaiming the Social Value of Privacy” in Kerr, Steeves & Lucock, *supra* note 1 (proposing “an alternative framework that conceptualizes privacy as a dynamic process of negotiating personal boundaries in intersubjective relations” at 193).

¹²² The difficulty in defining privacy is not troubling for some. See e.g. Fernando Volio, “Legal personality, privacy and the family” in Henkin, ed, *The International Bill of Rights* (New York: Columbia University Press, 1981) (“in one sense, all human rights are aspects of the right to privacy” at 184). Privacy is recognized in a number of international instruments, including in Article 12 of the *Universal Declaration of Human Rights*, GA Res 217 A (III), UN Doc A/810, at 71 (1948) (“No one shall be subjected to arbitrary interference with his privacy, family, home or correspondence, nor to attacks upon his honour and reputation”), Article 17 of the *International Covenant on Civil and Political Rights* 999 UNTS 171, and Article 8 of the *European Convention for the Protection of Human Rights and Fundamental Freedoms* 213 UNTS 221. See also *Convention on the Rights of the Child*, UNGA Doc A/RES/44/25 (12 December 1989) with Annex, art 16.

¹²³ See e.g. *BMG v Doe*, *supra* note 59 at para 4:

Citizens legitimately worry about encroachment upon their privacy rights. The potential for unwarranted intrusion into individual personal lives is now unparalleled. In an era where people perform many tasks over the Internet, it is possible to learn where one works, resides or shops, his or her financial information, the publications one reads and subscribes to and even specific newspaper articles he or she has browsed. This intrusion not only puts individuals at great personal risk but also subjects their views and beliefs to untenable scrutiny...

valued by civilized men,"¹²⁴ privacy finds protection in a variety of different forms in Canadian law. Indeed, although approaches to privacy regulation vary,¹²⁵ Canada is often cited as having a leading and influential global role in matters of privacy.¹²⁶ The following sections of this chapter provide a brief overview of privacy protections under the *Canadian Charter of Rights and Freedoms*,¹²⁷ common law and civil law, and legislation.¹²⁸

¹²⁴ *Olmstead v United States*, (1928) 227 US 438 at 478-79 (per Brandeis, J dissenting):

The makers of our Constitution [...] recognized the significance of man's spiritual nature, of his feelings and of his intellect. [...] They sought to protect Americans in their beliefs, their thoughts, their emotions and their sensations. They conferred, as against the Government, the right to be let alone – the most comprehensive of rights and the right most valued by civilized men. To protect that right, every unjustifiable intrusion by the Government upon the privacy of the individual, whatever the means employed, must be deemed a violation of the Fourth Amendment. And the use, as evidence in a criminal proceeding, of facts ascertained by such intrusion must be deemed a violation of the Fifth.

¹²⁵ See generally Solove & Rotenberg, *supra* note 13; Electronic Privacy Information Center, *Privacy and Human Rights Report 2006: An International Survey of Privacy Laws and Developments* (Washington: EPIC, 2007); Colin J Bennett, *Regulating Privacy: Data Protection and Public Policy in Europe and the United States* (Ithaca: Cornell University Press, 1992); Colin Bennett & Charles Raab, *The Governance of Privacy: Policy Instruments in Global Perspective*, 2d ed (Cambridge: MIT Press, 2006).

¹²⁶ See e.g. The Economist, "Legal Confusion on Internet Privacy: The Clash of Data Civilizations" (17 June 2010) *The Economist*, online: The Economist <www.economist.com/node/16377097>; Chantal Bernier, "Canada's Role and Influence in the Global Privacy Arena" (3 June 2011), online: OPC <www.priv.gc.ca/speech/2011/sp-d_20110603_cb_e_.cfm>.

¹²⁷ *Canadian Charter of Rights and Freedoms, Part I of the Constitution Act, 1982, being Schedule B to the Canada Act 1982 (U.K.)*, 1982, c 11 [Charter].

¹²⁸ It should be noted that the following sections of this chapter do not address, for example, the myriad privacy laws that govern the health sector or the public sector. See e.g. *Privacy Act*, RSC 1985, c P-21.

A. The Canadian Charter of Rights and Freedoms

Privacy is not explicitly recognized in the *Charter*. However, the Supreme Court of Canada (SCC) has frequently recognized a right to privacy inherent in sections 7 and 8 of the *Charter*. Section 7 of the *Charter* provides that “[e]veryone has the right to life, liberty and security of the person and the right not to be deprived thereof except in accordance with the principles of fundamental justice.” Section 8 states that “[e]veryone has the right to be secure against unreasonable search or seizure.”

In recognizing the right of privacy in the *Charter*, the SCC has stated that the protection of privacy is an “essential component of what it means to be free”¹²⁹ and that “[g]rounded in man’s physical and moral autonomy, privacy is essential for the well-being of the individual [...and] has profound significance for the public order.”¹³⁰ The SCC has also noted that if:

...the privacy of the individual is to be protected, we cannot afford to wait to vindicate it only after it has been violated. [...] Invasions of privacy must be prevented, and where privacy is outweighed by other societal claims, there must be clear rules setting forth the conditions in which it can be violated.¹³¹

Recognizing that privacy is “a broad and somewhat evanescent concept”¹³², however, the SCC has also attempted to articulate some of the distinct categories within the concept of privacy. In addition to a formulation of privacy that takes into account spatial and

¹²⁹ See e.g. *R v O’Connor*, [1995] 4 SCR 411 at paras 110-19; *Hunter v Southam*, [1984] 2 SCR 145 at 159.

¹³⁰ *R v Dyment*, *supra* note 13 at para 17.

¹³¹ *Ibid* at para 23. The need for clear rules is a need that this dissertation aims to help satisfy in the copyright context.

¹³² *Dagg v Canada (Minister of Finance)*, [1997] 2 SCR 403 at para 67.

bodily¹³³ privacy claims—which frequently arise in relation to police searches of places, property and persons, including requests for blood, urine, DNA, etc.—the Court has “ruptured the shackles that confined [privacy] claims to property”¹³⁴ and adopted a concept of informational privacy, noting that “[t]his too is based on the notion of the dignity and integrity of the individual.”¹³⁵ As a result, section 8 of the *Charter* now protects the following three distinct but potentially overlapping categories of privacy:

- (i) personal privacy, involving bodily integrity and the right not to have our bodies touched or explored;
- (ii) territorial privacy, involving varying expectations of privacy in the places we occupy, with privacy in the

¹³³ See e.g. *R v Pohoretsky*, [1987] 1 SCR 945.

¹³⁴ *R v Dymment*, *supra* note 13 at para 20, citing *Hunter v Southam Inc*, *supra* note 129 at 159.

¹³⁵ *R v Dymment*, *ibid* at para 22:

Finally, there is privacy in relation to information. This too is based on the notion of the dignity and integrity of the individual. As the Task Force put it (p. 13): “This notion of privacy derives from the assumption that all information about a person is in a fundamental way his own, for him to communicate or retain for himself as he sees fit.” In modern society, especially, retention of information about oneself is extremely important. We may, for one reason or another, wish or be compelled to reveal such information, but situations abound where the reasonable expectations of the individual that the information shall remain confidential to the persons to whom, and restricted to the purposes for which it is divulged, must be protected.

See also *R v Duarte*, [1990] 1 SCR 30 (“privacy may be defined as the right of the individual to determine for himself when, how, and to what extent he will release personal information about himself” at 46); *Schreiber v Canada (Attorney General)*, [1998] 1 SCR 841 (“privacy is closely linked to the effect that a breach of that privacy would have on the freedom and dignity of the individual” at para 19).

home attracting heightened protection because of the intimate and private activities taking place there;¹³⁶

(iii) informational privacy, involving “the claim of individuals, groups, or institutions to determine for themselves when, how, and to what extent information about them is communicated to others.”¹³⁷

Of course, the right to privacy under the *Charter* is not absolute. The *Charter* recognizes that there are a variety of circumstances where privacy should give way to other needs and interests. Section 8 protects individuals against *unreasonable* searches and seizures, not *all* searches and seizures. Put in the affirmative, the protection afforded by section 8 of the *Charter* applies only where an individual has a reasonable expectation of privacy, based on “the totality of the circumstances.”¹³⁸ In making this determination, Canadian courts ask (a) whether the individual had a subjective expectation of privacy and (b) whether that expectation of privacy was objectively reasonable.¹³⁹ Where an individual does not have a

¹³⁶ The fact that many forms of intellectual activities (e.g. reading and writing) take place in the home suggests that they should attract a heightened protection under an approach to privacy protection that is similar to the *Charter*. This point is revisited in Part III below.

¹³⁷ *R v Tessling*, *supra* note 13 at paras 23, 24, quoting Alan Westin, *Privacy and Freedom* (New York: Atheneum, 1970) at 7. See also *R v Gomboc*, 2010 SCC 55 at paras 19, 49 (more explicitly acknowledging the overlapping nature of these categories). For further discussion of information privacy, see e.g. Julie Cohen, “Examined Lives”, *supra* note 13 (discussing conceptions of informational privacy but noting that “privacy theory and privacy rhetoric do not know quite what to do with the notion of ‘informational privacy’” at 1375). For a description of the American legal approach to information privacy, see Solove & Rotenberg, *supra* note 13 at 184-92.

¹³⁸ *R v Edwards*, [1996] 1 SCR 128 at para 45.

¹³⁹ See *R v Tessling*, *supra* note 13 at para 19; *R v Kang-Brown*, 2008 SCC 18; *R v Patrick*, 2009 SCC 17.

reasonable expectation of privacy, section 8 of the *Charter* is not engaged.¹⁴⁰

In the informational privacy context in particular, the reasonable expectation of privacy test under the *Charter* normally asks whether the information at issue is “a biographical core of personal information [including] information which tends to reveal intimate details of the lifestyle and personal choices of the individual.”¹⁴¹ However, even where the information at issue does not fall within the “biographical core”, it may nevertheless attract a reasonable expectation of privacy.¹⁴² For example, communications may be protected if they are reasonably intended by their maker to be private, whether or not they disclose biographical core information.¹⁴³

Where individuals are found to have a reasonable expectation of privacy under the *Charter* as described above, courts will move to a second stage of analysis and ask whether the invasion of privacy is reasonable. For example, a search or seizure by the police will be reasonable if the police are authorized by a reasonable law to conduct the search or seizure and the search or seizure is in fact conducted in a reasonable manner.¹⁴⁴ “Search or seizure” in this

¹⁴⁰ *R v Patrick*, *ibid.*

¹⁴¹ *R v Plant*, [1993] 3 SCR 281 at 293:

This would include information which tends to reveal intimate details of the lifestyle and personal choices of the individual [and in determining whether a reasonable expectation of privacy exists, the court should consider] the nature of the information itself, the nature of the relationship between the party releasing the information and the party claiming its confidentiality, the place where the information was obtained, the manner in which it was obtained and the seriousness of the crime being investigated.

¹⁴² *R v AM*, 2008 SCC 19 at para 68. But see *R v Gomboc*, *supra* note 137.

¹⁴³ *Ibid.*

¹⁴⁴ *R v Collins*, [1987] 1 SCR 265 at 278.

context is used in a broad sense and includes any invasion of privacy in the three categories referenced above—i.e. a “search or seizure” may include searching a person (personal privacy) or a home (territorial privacy), or collecting information about an individual from any source (informational privacy). Even where there is no search *per se*, a ‘seizure’ (i.e. a collection) of information may give rise to a violation of section 8 of the *Charter*.¹⁴⁵

The curious reader unfamiliar with Canadian constitutional law might ask why it is necessary to articulate protection for any form of privacy in the copyright context, given the wide ranging privacy protections under the *Charter*. Part of the answer lies in the fact that the *Charter* applies only to government actors—i.e. to individuals’ interactions with the state—not directly to individuals’ interactions with copyright holders in the private sector.¹⁴⁶ The latter context requires consideration of privacy protections at common law¹⁴⁷ and civil law and under legislation that governs the private sector, each of which is discussed below.

¹⁴⁵ See e.g. *R v Dymment*, *supra* note 13 at para 25:

In this case, [...] there was no search. The doctor simply collected the blood as it flowed from an open wound and it was later handed over by him to the police officer. It should be observed, however, that s. 8 of the Charter does not protect only against searches, or against seizures made in connection with searches. It protects against searches or seizures.

¹⁴⁶ Yet, it should be noted that it is a well-established principle of Canadian law that the common law should be interpreted in a manner which is consistent with *Charter* principles. See *Hill v Church of Scientology of Toronto*, [1995] 2 SCR 1130 at 1169; *M (A) v Ryan*, [1997] 1 SCR 157; *Dagenais v CBC* [1994] 3 SCR 835 at 875-78; *R v Salituro*, [1991] 13 SCR 654 at 671. See generally John Craig, “Invasion of Privacy and Charter Values: The Common Law Tort Awakens” (1997), 42 McGill LJ 355.

¹⁴⁷ Canada has not yet expressly recognized a freestanding claim of ‘invasion of privacy’. A number of commentators have argued that such a tort should be created. See e.g. Robyn M Ryan Bell, “Tort of Invasion of Privacy – Has its

For the purposes of this dissertation, it is notable that the SCC has expressly observed that interference (of the kind described in Chapter 1 and further discussed in Chapter 3 below) with intellectual privacy implicates precisely the class of information—biographical core information—that is protected under the *Charter*.¹⁴⁸ In *Society of Composers, Authors and Music Publishers of Canada v Canadian Assn. of Internet Providers*¹⁴⁹, LeBel, J. stated that:

...monitoring of an individual's surfing and downloading activities [...] tend[s] 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 user's downloading of copyrighted works. We should therefore be chary of adopting a test that may encourage such monitoring.¹⁵⁰

In *SOCAN v CAIP* LeBel, J. asserted that the Court should adopt an interpretation of the *Copyright Act* that respects individuals' privacy interests in connection with their internet surfing and downloading activities. That suggestion is certainly in keeping with the arguments proposed in this dissertation and, along with other concepts, values and principles that emerge from *Charter* jurisprudence,¹⁵¹ forms part of the analysis of possible solutions explored in Chapter 5.¹⁵²

Time Finally Come?" in Todd Archibald & Michael Cochrane, *Annual Review of Civil Litigation* (Toronto: Thomson Carswell, 2005); Craig, *ibid*.

¹⁴⁸ See also *supra* note 138 and accompanying text.

¹⁴⁹ *SOCAN v CAIP*, *supra* note 59.

¹⁵⁰ *Ibid* at para 155.

¹⁵¹ For example, see *R v Cross*, 2007 CanLII 64141 (ONSC) ("In my view the very nature of a 'personal computer' places it and the data it contains within the biographical core of personal information which individuals in a free and democratic society would wish to maintain and control from dissemination to the state" at para 2), which has obvious implications for intellectual privacy

In addition, in a number of cases courts have reinforced the notion that information contained on personal computers, including internet browsing history, engages precisely the kind of privacy interests that are protected by the *Charter*.¹⁵³ Searches of personal computers are “potentially among the most invasive of searches.”¹⁵⁴ In *R v Morelli*, for example, the SCC stated that an individual’s personal internet browsing history is “the electronic roadmap of your cybernetic peregrinations, where you have been and what you appear to have seen on the Internet.”¹⁵⁵ Fish, J. stated the following for the majority of the Court:

It is difficult to imagine a search more intrusive, extensive, or invasive of one’s privacy than the search and seizure of a personal computer.

First, police officers enter your home, take possession of your computer, and carry it off for examination in a place unknown and inaccessible to you. There, without supervision or constraint, they scour the entire contents

because in the information age individuals access and enjoy many forms of copyright works using a personal computer. See also *R v Cole*, 2011 ONCA 218 (finding that a teacher had a reasonable expectation of privacy in the contents of a work computer on which he was entitled to store personal information, in part because “[t]here was no clear and unambiguous policy to monitor, search or police the teachers’ use of their laptops” at para 45).

¹⁵² See e.g. *ibid*. It must be acknowledged that such statements about the impact of the *Charter* do not appear to have had a significant impact in the private sector, particularly in the employment context. See generally Michael Geist, *Computer and E-mail Workplace Surveillance in Canada: The Shift from Reasonable Expectation of Privacy to Reasonable Surveillance* (Ottawa: Canadian Judicial Council, 2002) at 41, online: Canadian Judicial Council <http://www.cjccm.gc.ca/cmslib/general/news_pub_techissues_Surveillance_2002_en.pdf>; Melanie R Bueckert, *The law of employee monitoring in Canada* (Markham: LexisNexis, 2009).

¹⁵³ See e.g. *R v Cross*, *supra* note 151; *R v Cole*, *supra* note 151 at paras 33-48.

¹⁵⁴ *R v Cole*, *ibid* at para 86.

¹⁵⁵ *R v Morelli*, 2010 SCC 8 at para 3.

of your hard drive: your emails sent and received; accompanying attachments; your personal notes and correspondence; your meetings and appointments; your medical and financial records; and all other saved documents that you have downloaded, copied, scanned, or created. The police scrutinize as well the electronic roadmap of your cybernetic peregrinations, where you have been and what you appear to have seen on the Internet – generally by design, but sometimes by accident.¹⁵⁶

Again, the foregoing analysis under the *Charter* is consistent with the arguments presented in this dissertation regarding the definition of intellectual privacy, including the values that are interrelated with that concept.

B. Common Law and Civil Law¹⁵⁷

Unlike the relatively well-developed *Charter* right to privacy, Canadian common law jurisprudence is largely equivocal about whether, or to what extent, the common law protects privacy interests.¹⁵⁸ It has been suggested that a separate tort of invasion of

¹⁵⁶ *Ibid* at paras 2, 3.

¹⁵⁷ Portions of this section are derived in part from Alex Cameron & Mimi Palmer, “Invasion of Privacy as a Common Law Tort in Canada” (2009) 6 Canadian Privacy Law Review 105.

¹⁵⁸ See generally GHL Fridman, *The Law of Torts in Canada*, 2d ed (Toronto: Carswell, 2002) (describing this struggle as the courts “groping their way towards” a tort for invasion of privacy at 20-21). See also *Ontario (Attorney-General) v Dieleman*, [1994] 117 DLR (4th) 449 (“invasion of privacy in Canadian common law continues to be an inceptive, if not ephemeral, legal concept, primarily operating to extend the margins of existing tort doctrine” at para 568). Similarly, in the United States where common law privacy protections are far more developed than in Canada, it has been noted that:

Compared with common law privacy rights, constitutional privacy rights manifest far greater concern with intellectual privacy. The drafters of the Constitution were concerned with

privacy is neither necessary nor desirable.¹⁵⁹ Canadian courts have certainly been reluctant to confirm or deny the existence of invasion of privacy as a freestanding tort.¹⁶⁰ Instead, privacy interests have historically been principally addressed through legislative interventions and indirectly through the application of other torts, including appropriation of personality¹⁶¹, passing off, nuisance, harassment, wilful infliction of nervous suffering, defamation, breach of confidence, and injurious falsehood.¹⁶² Many early cases

safeguards against government overreaching, and so constitutional protections for intellectual privacy have no direct application to the practices of private information providers.

Cohen, “DRM and Privacy”, *supra* note 3 at 591.

¹⁵⁹ See e.g. Lewis N Klar, *Tort Law*, 4th ed, (Thomson Carswell: Toronto, 2008) at 84-87. See also John G Fleming, *The Law of Torts*, 6th ed (Sydney: Law Book Co, 1983) at 601-02; *Ontario (Attorney-General) v Dieleman*, *supra* note 158 (observing that “[d]ifficulties arise in determining the degree to which the law can reasonably protect the sensibilities of society without encouraging unmanageable subjective claims inconsistent with the close quarters in which we live” at 553).

¹⁶⁰ See generally Linden, *supra* note 116 (“[a]lthough the right to privacy is well-entrenched in American tort law, the Canadian and English courts have been reluctant to recognize a separate right to privacy” at 56). See also *Krouse v Chrysler Canada Ltd* [1970] 3 OR 135 (HCJ) (preliminary motion) [*Krouse- HCJ*], [1972] 2 OR 133 (HCJ) [*Krouse-OSC*], *aff’d* [1974] 1 OR (2d) 225 (CA).

¹⁶¹ See e.g. *Salé v Barr*, 2003 ABQB 431; *Racine v CJRC Radio Capitale Ltee*, 17 OR (2d) 370; *Corlett-Lockyer v Stephens*, [1996] BCJ No 857 [Prov Ct.]; *Horton v Tim Donut Ltd*, [1997] OJ No 390.

¹⁶² See generally Fridman, *supra* note 158 at 20-21. Privacy interests are also protected in other specific ways, including in the context of civil litigation. The deemed undertaking rule, for example, is based on a recognition by Canadian courts of the general right of privacy that a person has with respect to his or her own documents. See generally Paul Matthews & Hodge M Malek, *Discovery* (London: Sweet & Maxwell, 1992) at 253, cited in *Goodman v Rossi*, [1995] OJ No 1906 (CA) at para 29; *Tanner v Clark*, 2003 CanLII 41640 (Ont CA); *Royal Bank of Canada v Bacon* (1999), 218 NBR (2d) 98 (QB); *Vitapharm Canada Ltd v F Hoffmann-La Roche Ltd.*, [2002] OJ No 1400 (SC). See also Alex Cameron & Andrew Teehan, “New Rules of Civil Procedure and Recent Caselaw Highlight Privacy Themes in Civil Litigation” (2009) 6 Canadian

involved disputes between neighbours.¹⁶³ None of the early cases involved the use or disclosure of personal information that had been collected for a business purpose.¹⁶⁴

More recently, some Canadian courts have hinted at the possible emergence of a freestanding common law tort of invasion of privacy. In the 1996 decision in *Dyne Holding Ltd v Royal Insurance Co of Canada*,¹⁶⁵ for example, the P.E.I. Supreme Court, Appeal Division stated that, “[i]t would seem that courts in Canada are not far from recognizing a common law right of privacy if they have not already done so.”¹⁶⁶ Consistent with the evolution of the

Privacy Law Review 129; *Riddick v. Thames Board Mills Ltd*, [1977] 3 All ER 677 (CA) at 687 (per Lord Denning).

¹⁶³ For example, in *Roth v Roth* (1991), 4 OR (3d) (Gen Div), the defendants locked a gate on an access road to the plaintiffs’ cottage and shut off electricity in the cottage at a time when the plaintiffs were not there. The Court concluded that an invasion of privacy had occurred, but due to the overlapping nature of the cause of action of privacy with the tort of harassment, awarded damages as a lump sum without specifying that a particular portion of the damages was attributable to the invasion of privacy. In *Lipiec v Borsa* [1996] OJ No 3819, the Court held that the plaintiffs’ removal of a fence and installation of a surveillance camera directed at the defendants’ property constituted an intentional invasion of the defendants’ privacy. Finally, in *Saelman v Hill* [2004] OJ No 2122, the court stated (at paragraph 36) that, in some cases, invasion of privacy could be understood as a manifestation of the tort of nuisance:

I am of the view that the tort of nuisance is made out in circumstances where a neighbour deliberately, significantly and unjustifiably interferes with another neighbour's enjoyment of his or her property. This type of conduct may be labelled as harassment, intimidation or invasion of privacy and in my view, are in essence manifestations of the well-established tort of nuisance.

¹⁶⁴ Linda D Rainaldi, *Remedies in Tort* (Toronto: Carswell, 2000) at 24-12.2 to 24-12.4.

¹⁶⁵ *Dyne Holding Ltd v Royal Insurance Co of Canada* [1996] PEIJ No 28 (SC (AD)).

¹⁶⁶ *Ibid* at para 63.

Charter right to privacy, the common law has begun to grapple with privacy interests that are informational, not territorial, in nature.

In *Somwar v McDonald's Restaurants of Canada Limited*,¹⁶⁷ for example, the plaintiff alleged that the defendant unlawfully invaded his privacy by conducting a credit bureau check on him without his permission. The defendant sought to strike the claim as disclosing no reasonable cause of action. The Court reviewed Prosser's four categories of privacy interests, which form the basis of American privacy tort law,¹⁶⁸ and considered Fridman's¹⁶⁹ analysis of cases where Canadian courts have awarded damages in privacy-related cases.¹⁷⁰ The Court refused to strike the claim, finding that "it is not settled law in Ontario that there is no tort of invasion of privacy."¹⁷¹ In *obiter*, the Court went on to provide a strong endorsement for the recognition of invasion of privacy as a common law tort:

¹⁶⁷ *Somwar v McDonald's Restaurants of Canada Limited* (2006), 79 OR (3d) 172 (Ont SC) [*Somwar*].

¹⁶⁸ William L Prosser, "Privacy" (1960) 48 Cal L Rev 383 at 388-89:

(1) Intrusion upon the plaintiff's seclusion or solitude, or into his private affairs. (2) Public disclosure of embarrassing private facts about the plaintiff. (3) Publicity which places the plaintiff in a false light in the public eye. (4) Appropriation, for the defendant's advantage, of the plaintiff's name or likeness.

¹⁶⁹ Fridman, *supra* note 158.

¹⁷⁰ With Prosser and Fridman's remarks in mind, the Court surveyed the following nine Ontario cases where the question of invasion of privacy had arisen in a variety of different circumstances: *Capan v Capan*, [1980] OJ No 1361 (HCJ), cited *Roth v Roth*, *supra* note 163, *Saccone v Orr* (1981), 34 OR (2d) 317 (Co Ct), *Lipiec*, *supra* note 163, *Tran v Financial Debt Recovery Ltd*, [2000] OJ No 4293 (SCJ) rev'd on other grounds, [2001] OJ No 4103 (Div Ct), *Garrett v Mikalachki*, [2000] OJ No 1326 (SCJ), *Rathmann v Rudka*, [2001] OJ No 1334 (SCJ), *Haskett v Trans Union of Canada Inc.* (2001), 10 CCLT (3d) 128 (Ont SCJ), aff'd 15 CCLT (3d) 194, (Ont CA), and *TW v Seo*, [2003] OJ No 4277 (Ont SCJ) varied on other grounds at [2005] OJ No 2467 (CA).

¹⁷¹ *Somwar*, *supra* note 167 at para 22.

With advancements in technology, personal data of an individual can now be collected, accessed (properly and improperly), and disseminated more easily than ever before. There is a resulting increased concern in our society about the risk of unauthorized access to an individual's personal information. The traditional torts such as nuisance, trespass, and harassment may not provide adequate protection against infringement of an individual's privacy interests. Protection of those privacy interests by providing a common law remedy for their violation would be consistent with Charter values and an 'incremental revision' and logical extension of the existing jurisprudence. [...] Even if the plaintiff's claim for invasion of privacy were classified as 'novel' [...] the foregoing analysis leads me to conclude that the time has come to recognize invasion of privacy as a tort in its own right.¹⁷²

Somwar has been cited in a number of privacy-related cases since its release and for a time it appeared that courts (in Ontario at least) were nearing the point where a freestanding tort of invasion of privacy might be recognized.¹⁷³ However, the recent decision in *Jones v Tsige*¹⁷⁴ suggests otherwise.

¹⁷² *Ibid* at paras 29, 31. The Court also commented at paragraphs 11-12 of the decision that invasion of privacy, if it is to be recognized, appears to be an intentional tort.

¹⁷³ See e.g. *Shred-Tech Corp v Viveen*, [2006] OJ No 4893 (SCJ). The Small Claims Court in Ontario has on one occasion purported to recognize invasion of privacy as a tort, including setting out the elements of the tort. See *Caltagirone v Scozzari-Cloutier*, [2007] OJ No. 4003 (SCJ). In addition, invasion of privacy as an independent tort was addressed twice in 2008: first in *Nitsopoulos v Wong*, [2008] OJ No 3498 (SCJ) and later in *Warman v Grosvenor*, [2008] OJ No 4462 (SCJ). However, like *Somwar*, neither case was determinative of the issue.

¹⁷⁴ *Jones v Tsige*, 2011 ONSC 1475. The author was counsel to the defendant in this case.

The facts in *Jones v. Tsige* involved a claim against an employee of a bank who repeatedly viewed a co-worker's banking records without authorization over a number of years. The bank investigated the incident and disciplined the defendant. The plaintiff brought an action against the defendant for invasion of privacy but did not sue the bank.

In *Jones v Tsige*, Whitaker, J. canvassed the jurisprudence, including *Somwar*, and concluded that there is no common law tort of invasion of privacy in Ontario.¹⁷⁵ The principal basis for the finding was the Ontario Court of Appeal's statement in *Euteneier v. Lee*¹⁷⁶ that "...there is no 'free standing' right to dignity or privacy under the *Charter* or at common law..."¹⁷⁷ That statement had not been squarely addressed in *Somwar* or any of the other privacy-related cases decided since *Euteneier*. In addition, the defendant in *Jones v. Tsige* argued that the legislature, not the court, was the appropriate venue for making any decision(s) about whether and how to regulate privacy, particularly given the numerous stakeholder interests and the tremendous amount of legislative activity that had already taken place with respect to privacy in Canada.¹⁷⁸ Although those arguments were not ultimately determinative, the Court clearly considered the existence of the numerous legislative regimes to be a relevant consideration:

Turning back now to the various statutory provisions that govern privacy issues, most Canadian jurisdictions have statutory administrative schemes that govern and regulate privacy issues and disputes. In Ontario, it cannot be said that there is a legal vacuum that permits wrongs to go unrighted - requiring judicial intervention. [...]

¹⁷⁵ *Ibid* at para 57.

¹⁷⁶ *Euteneier v Lee* [2005] 77 OR (3d) 621; 260 DLR (4th) 145 (Ont CA).

¹⁷⁷ *Ibid* at para 63.

¹⁷⁸ *Jones v Tsige*, *supra* note 174 (Factum of the Defendant at paras 43-56).

I would also note that this is not an area of law that requires judge-made rights and obligations. Statutory schemes that govern privacy issues are, for the most part, carefully nuanced and designed to balance practical concerns and needs in an industry-specific fashion.

I conclude that there is no tort of invasion of privacy in Ontario.¹⁷⁹

At the time of writing, *Jones v. Tsige* had been appealed and the Ontario Court of Appeal had reserved its decision.

Four Canadian provinces have created a statutory tort of invasion of privacy: British Columbia, Manitoba, Newfoundland and Saskatchewan.¹⁸⁰ Courts in these provinces have generally (though not uniformly) rejected any notion that there is an independent tort of invasion of privacy at common law.¹⁸¹ In a number of cases,

¹⁷⁹ *Ibid* at paras 53-57.

¹⁸⁰ *Privacy Act*, RSBC 1996, c 373 (“BC Privacy Act”); *The Privacy Act*, RSS 1978, c P-24; *The Privacy Act*, CCSM c P125; *Privacy Act*, RSNL 1990, c P-22.

¹⁸¹ See e.g. *Hung v Gardiner*, 2002 BCSC 1234 at para 110, *aff’d* 2003 BCCA 257 (rejecting the existence of a common law tort of invasion of privacy); *Bracker v Vancouver (City) Police Board*, [2006] BCJ No 233; *Peters Brown v Regina District Health Board* [1995] SJ No 609; *Koeppen v LoVecchio*, [2001] AJ No 619; *Brown v Bermax Capital Ltd.* [1998] MJ No 296; *Lord v Canada (Attorney General)*, [2000] BCJ No 1206 (BCSC); *Mohl v University of British Columbia*, 2009 BCCA 249 (“There is no common-law claim for breach of privacy. The claim must rest on the provisions of the [BC Privacy Act]” at para 13). For a particularly strong rejection of the idea that there is a common law tort for invasion of privacy from an appellate court, see *Bingo Enterprises Ltd et al v Plaxton et al* (1986), 26 DLR (4th) 604 (Man CA). In one Newfoundland case, however, the Court did not rule out the possibility that the common law may protect privacy in addition to the statutory tort: see *Gibson v National Association of Broadcast Employees and Technicians*, [1983] NJ No 262 (Nfld SC). The Court in *Dawe v Nova Scotia Collection Services (Nfld) Ltd* [1998] NJ No 22 (Nfld Prov Ct) went a step further and held that a common law action for invasion of privacy was not precluded by the legislation.

courts in these provinces have indicated that if there is a right to sue for invasion of privacy, that right is found under the relevant statutory tort in the province.¹⁸² Outside of the above provinces, including in Ontario as discussed above, Canadian courts have been inconclusive about whether the common law includes an independent tort of invasion of privacy.¹⁸³

In sharp contrast to the unsettled state of privacy at common law, however, privacy claims have fared well in Québec under the *Québec Charter*¹⁸⁴ and the *Civil Code of Québec*.¹⁸⁵ Privacy is central to the civil law tradition of personality rights, based on concept of

¹⁸² See e.g. *Bracker v Vancouver*, *ibid*; *Peters Brown v Regina District*, *ibid*; *Brown v Bermex*, *ibid*. But see *Gibson v National Association of Broadcast Employees and Technicians*, *ibid*; *Dawe v Nova Scotia Collection Services (Nfld) Ltd*, *ibid*.

¹⁸³ See e.g. *French v Dalhousie University*, [2003] NSJ No 44; *Koeppen v LoVecchio*, *supra* note 181; *Motherwell v Motherwell*, [1977] AJ No 660 (extending the tort of nuisance to cover privacy).

¹⁸⁴ *Québec Charter of Human Rights and Freedoms*, RSQ, c C-12 [*Quebec Charter*]: ("Every person has a right to respect for his private life," s 5).

¹⁸⁵ *Civil Code of Québec*, SQ 1991, c 64, arts 35, 36:

35. Every person has a right to the respect of his reputation and privacy. No one may invade the privacy of a person without the consent of the person or his heirs unless authorized by law.

36. The following acts, in particular, may be considered as invasions of the privacy of a person:

- (1) entering or taking anything in his dwelling;
- (2) intentionally intercepting or using his private communications;
- (3) appropriating or using his image or voice while he is in private premises;
- (4) keeping his private life under observation by any means;
- (5) using his name, image, likeness or voice for a purpose other than the legitimate information of the public;
- (6) using his correspondence, manuscripts or other personal documents.

dignity.¹⁸⁶ More than a decade ago, the SCC released its landmark judgment in *Aubry v Éditions Vice-Versa Inc.*,¹⁸⁷ a decision on invasion of privacy involving the unauthorized publication of a photograph of a young woman. Notwithstanding that the woman was photographed sitting in a public place (that some might consider should attract little or no expectation of privacy), the court awarded \$2,000 in damages for invasion of privacy. The *Aubry* case is also notable for the purposes of this dissertation because it pitted the right of the artist to publish the work against the right of privacy of the individual subject of the work:

An artist's right to publish his or her work cannot include the right to infringe, without any justification, a fundamental right of the subject whose image appears in the work. While the artist's right must be taken into consideration, so must the rights of the photograph's subject. If it is accepted that publishing the artist's work is an exercise of freedom of expression, the respondent's right not to consent must also be taken into consideration.¹⁸⁸

Privacy claims continue to be successfully advanced in Québec, including in insurance cases where inappropriate surveillance has resulted in significant damage and punitive damage awards.¹⁸⁹

¹⁸⁶ See generally Louis LeBel, "La Protection des Droits Fondamentaux et la Responsabilité Civile" (2004) 49 McGill LJ 231.

¹⁸⁷ *Aubry v Éditions Vice-Versa Inc.*, [1998] 1 SCR 591 [*Aubry*].

¹⁸⁸ *Ibid* at para 63. Query whether the court would have reached the same decision if the case had been brought under *PIPEDA*. Paragraph 4(2)(c) of *PIPEDA* provides that the legislation does not apply to "any organization in respect of personal information that the organization collects, uses or discloses for journalistic, artistic or literary purposes and does not collect, use or disclose for any other purpose." *PIPEDA*, *supra* note 13.

¹⁸⁹ See e.g. *Veilleux c Compagnie d'assurance-vie Penncorp*, 2008 QCCA 257; *Compagnie d'assurances Standard Life c Tremblay*, 2010 QCCA 933.

Further, in *Loranger v. Cote*¹⁹⁰, the court awarded \$1,000 in moral damages in a case where the defendant took a nude photograph of the plaintiff and provided it to a magazine (which later published the photograph) without the plaintiff's permission. Although the plaintiff was not identifiable in the photograph, the court held that the defendant had nevertheless invaded the plaintiff's privacy. In *G(J) v. B(M)*¹⁹¹, the defendant published photographs and videos on the Internet that depicted his former girlfriend, the plaintiff, nude and engaged in sexual activity. The court awarded the plaintiff \$20,000 in moral damages and \$10,000 in exemplary damages.

C. Privacy Legislation

1. First Generation: Statutory Torts¹⁹²

As mentioned in the preceding section, four Canadian provinces have enacted statutory torts of 'invasion of privacy'.¹⁹³ Since these laws are virtually identical to one another, it suffices for our purposes to briefly review one of them: the *BC Privacy Act*. That law was enacted in 1968 following a controversy over electronic eavesdropping during a trade union convention and was the first law of its kind.¹⁹⁴

¹⁹⁰ *Loranger v Cote*, No CQ Montreal 500-32-106905-070 (CQ) (May 20, 2009).

¹⁹¹ *G(J) v B(M)*, 2009 CarswellQue 6241 (Que SC).

¹⁹² Other 'first generation' privacy laws include the *Privacy Act*, *supra* note 128 enacted in 1982 and the *Access to Information Act*, RSC 1985, c A-1. Such laws, and their provincial equivalents, are designed to protect individuals' privacy with respect to information held by government institutions and to provide individuals with a right of access to that information. These laws are not explored in this chapter. Nor are other laws and rules that contain privacy-related provisions, including the *Consumer Reporting Act*, RSO 1990, c C33.

¹⁹³ See *supra* note 180 and accompanying text.

¹⁹⁴ British Columbia Law Institute, *Report on the Privacy Act of British Columbia* (Vancouver: BCLI report no 49, 2008) at 1-2, citing RA Sargent

Under the *BC Privacy Act*, it is a tort “actionable without proof of damage, for a person, willfully and without a claim of right, to violate the privacy of another.”¹⁹⁵ Like the *Charter*, the *BC Privacy Act* provides that individuals are entitled to a reasonable expectation of privacy.¹⁹⁶ Among other things, the “nature, incidence and occasion” of the act complained of must be considered.¹⁹⁷ The *BC Privacy Act* also includes a number of statutory defences. For example, it states that an act is not a violation of privacy if it is consented to,¹⁹⁸ if it was incidental to a lawful defence of person or property,¹⁹⁹ if it was authorized or required by law or a court,²⁰⁰ or if it was a publication of a matter that was fair comment or in the public interest.²⁰¹

Notwithstanding the potentially wide application and remedies under the provincial statutory torts, in the decades since they were enacted, relatively few cases have proceeded under the provincial statutory torts; in only a few of those cases have plaintiffs been successful.²⁰²

(Commissioner), *Report of the Royal Commission of Inquiry into Invasion of Privacy* (Victoria: The Queen’s Printer, 1967) at 5-9.

¹⁹⁵ *BC Privacy Act*, *supra* note 180, s 1(1). The legislation also contains special rules for privacy rights in connection with the use of personal portraits.

¹⁹⁶ *Ibid*, at s 1(2) (“The nature and degree of privacy to which a person is entitled in a situation or in relation to a matter is that which is reasonable in the circumstances, giving due regard to the lawful interests of others.”)

¹⁹⁷ *Ibid*, s 1(3). The Court must also consider “any domestic or other relationship between the parties”.

¹⁹⁸ *Ibid*, s 2(2)(a).

¹⁹⁹ *Ibid*, s 2(2)(b).

²⁰⁰ *Ibid*, s 2(2)(c).

²⁰¹ *Ibid*, s 2(3).

²⁰² See e.g. British Columbia Law Institute, *supra* note 194 (“In the nearly forty years since it was enacted, relatively few cases have been decided under the provincial *Privacy Act*, and very few actions have succeeded” at 22).

2. Second Generation: Data Protection Legislation²⁰³

In response to the European data protection directive²⁰⁴ and in an attempt to support and promote electronic commerce, in the late 1990s the Canadian government enacted *PIPEDA*.²⁰⁵ *PIPEDA* was implemented in phases over a three-year period that began on January 1, 2001. *PIPEDA* has been approved by the European Community as providing adequate protection.²⁰⁶

Consistent with many other data protection laws around the world,²⁰⁷ *PIPEDA* is a privacy law that provides individuals with the right to control the collection, use and disclosure of information

²⁰³ Portions of the background material in this section are derived in part from passages written by the author for the OPC which appear in *Leading by Example: Key Developments in the First Seven Years of the Personal Information Protection and Electronic Documents Act (PIPEDA)* (2008), online: OPC <http://www.priv.gc.ca/information/pub/lbe_080523_e.cfm> [OPC, *Leading by Example*].

²⁰⁴ EC, *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*, [1995] OJ L 281/31 [EU Data Protection Directive].

²⁰⁵ *PIPEDA*, *supra* note 13. The full title of the legislation is: *An Act to support and promote electronic commerce by protecting personal information that is collected, used or disclosed in certain circumstances, by providing for the use of electronic means to communicate or record information or transactions and by amending the Canada Evidence Act, the Statutory Instruments Act and the Statute Revision Act*.

²⁰⁶ The Commission of the European Communities issued Decision 2002/2/EC pursuant to art 25(6) of EU Data Protection Directive, *supra* note 204 which 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*. EC, 2002/2/EC: *Commission Decision of 20 December 2001 pursuant to Directive 95/46/EC of the European Parliament and of the Council on the adequate protection of personal data provided by the Canadian Personal Information Protection and Electronic Documents Act (notified under document number C(2001) 4539)* [2002] OJ, L 2 at 13.

²⁰⁷ See e.g. *Federal Data Protection Act (Bundesdatenschutzgesetz)*, adopted 18 May 2001, published in the *Bundesgesetzblatt I* Nr 23/2001, 904 on 22 May 2001.

about them by granting, refusing or withdrawing consent. *PIPEDA* expressly incorporates the Canadian Standards Association *Model Code for the Protection of Personal Information*,²⁰⁸ developed by consensus in 1995 and which represents the culmination of many years of research, review and debate by and among a large number of public sector and private sector stakeholders.²⁰⁹

Subject to the exceptions described in the paragraph below, *PIPEDA* applies to every organization in respect of personal information that the organization collects, uses or discloses in the course of commercial activities. *PIPEDA* also applies to federal works, undertakings and businesses in respect of employee personal information that they collect, use or disclose in connection with their operations, whether or not a commercial activity is involved.

PIPEDA does not apply to an organization in respect of personal information that the organization collects, uses or discloses within Alberta, British Columbia or Quebec, (or within Ontario, in respect of personal health information collected, used or disclosed by health information custodians governed by Ontario's *Personal Health Information Protection Act*²¹⁰) unless: (a) the organization is a federal work, undertaking or business; or (b) the personal information is disclosed outside of the province in the course of a commercial activity. These provinces have enacted privacy laws that have been declared substantially similar to *PIPEDA*.²¹¹ As a result, the collection, use or disclosure of personal information by

²⁰⁸ *CSA Model Code*, supra note 13. The *CSA Model Code* was based in part on the *OECD Guidelines*, supra note 13.

²⁰⁹ *Englander v TELUS Communications Inc*, [2005] 2 FCR 572 (CA) at paras 8-17; see also *McIsaac, Shields & Klein*, supra note 113 at 4-31-32.

²¹⁰ *Personal Health Information Protection Act*, 2004, SO 2004, c 3, Sch A.

²¹¹ *An Act Respecting the Protection of Personal Information in the Private Sector*, RSQ c P-39.1; *Personal Information Protection Act*, SBC 2003 c 63 [BC PIPA]; *Personal Information Protection Act*, SA 2003, c P-6.5; *ibid*.

organizations in the course of commercial activities in these provinces is subject to the applicable provincial laws, not *PIPEDA*, except as provided in (a) and (b) above. *PIPEDA* applies to organizations' commercial activities in all other provinces.

PIPEDA only applies to the collection, use and disclosure of "personal information." This term is broadly defined in subsection 2(1) as "information about an identifiable individual", excluding "the name, title or business address or telephone number of an employee of an organization." Notably, unlike the privacy protections afforded under the *Charter* and statutory torts (and the common law, should it recognize such a tort), privacy protection under *PIPEDA* does not depend upon the concept of "reasonable expectation of privacy."²¹² While consent may be implied in certain circumstances, such circumstances are relatively narrow.

Generally speaking, *PIPEDA* requires organizations to comply with a set of legal obligations that are based on the following ten principles: (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, and (10) Challenging compliance. Sub-section 5(3) of *PIPEDA* contains an over-arching requirement that organizations may only collect, use or disclose personal information for purposes that a reasonable person would consider appropriate in the circumstances.²¹³

The role of the OPC under *PIPEDA* is to investigate complaints, make findings and issue non-binding recommendations where appropriate. An individual complainant or the OPC may then proceed to Federal Court to seek legal enforcement in certain cases,

²¹² But see Part I of Chapter 5.

²¹³ This requirement is considered in more detail in Chapter 5. It arguably invites the introduction of "reasonable expectations" of privacy into the analysis under *PIPEDA*, a topic which is also revisited in Chapter 5.

including damages. The OPC has issued hundreds of findings under *PIPEDA* and the Federal Court has issued numerous decisions.

While none of the decisions issued to-date under *PIPEDA* directly implicates intellectual privacy interests,²¹⁴ it must be acknowledged that *PIPEDA*, being primarily concerned with informational privacy, can and does apply to a number of practices that diminish intellectual privacy.²¹⁵ Indeed, the application of *PIPEDA* to particular DRM-related practices that implicate intellectual privacy is considered in detail in Chapter 5.

3. Third Generation: Sector-Specific Laws

PIPEDA is a regulatory instrument of general application that many in Canada consider has proved remarkably resilient in adapting to the myriad new technologies and business practices that have emerged over the past decade since it was enacted.²¹⁶ However, notwithstanding that *PIPEDA* and its provincial equivalents apply to virtually all private sector activities, Canada has also seen the emergence of a variety of sector- or activity-specific privacy laws over the past decade.²¹⁷ For example, specialized laws and rules have been created to address privacy in the health sector²¹⁸, and in the context of telemarketing²¹⁹ and anti-

²¹⁴ For further discussion, see Chapter 5.

²¹⁵ CIPPIC, “Digital Rights Management and Consumer Privacy”, *supra* note 30.

²¹⁶ The legislation is subject to review by Parliament every five years.

²¹⁷ By contrast, the United States has enacted almost exclusively sector-specific privacy laws, including the following: *Video Privacy Protection Act*, *supra* note 20; *Fair Credit Reporting Act (FCRA)*, 15 USC § 1681, *Cable TV Privacy Act of 1984*, 47 USC Sec 551, *Health Insurance Portability and Accountability Act (HIPAA)* of 1996 (PL104-191); *Children’s Online Privacy Protection Act of 1998 (COPPA)* (PL 105-277, 112 Stat 2681).

²¹⁸ See e.g. *Personal Health Information Protection Act*, *supra* note 210.

spam.²²⁰ For the purposes of this dissertation, these recent laws are interesting because, unlike *PIPEDA* which takes a general approach to privacy regulation, the more recent laws contain comparatively detailed rules and regulations. As discussed in Chapter 5, this may suggest that a similar approach can and perhaps should be taken in the specific context of intellectual privacy and copyright law.

In addition, Canada's forthcoming anti-spam law (*CASL*) contains detailed provisions that will have a direct impact on certain DRM-related activities that implicate intellectual privacy as described herein. For example, section 8 of *CASL* provides that organizations are prohibited from installing computer programs (which may in some cases include components of DRM systems) unless express consent has been obtained.

Section 10 of *CASL* dictates that such requests for express consent must set out "clearly and simply" the purpose(s) for which the consent is requested, as well as any information prescribed in the regulations, including information that identifies the person seeking the consent. The regulations under *CASL* are expected to set out in detail the additional forms of information that must be included.²²¹ Section 10 also requires that the request for consent

²¹⁹ See e.g. Canadian Radio-television and Telecommunications Commission (CRTC) *Unsolicited Telecommunications Rules* (20 July 2010) online: CRTC <<http://www.crtc.gc.ca/eng/trules-reglest.htm>>.

²²⁰ *An Act to promote the efficiency and adaptability of the Canadian economy by regulating certain activities that discourage reliance on electronic means of carrying out commercial activities, and to amend the Canadian Radio-television and Telecommunications Commission Act, the Competition Act, the Personal Information Protection and Electronic Documents Act and the Telecommunications Act*, SC 2010, c 23 E-1.6 [Assented to December 15, 2010] [*CASL*].

²²¹ At the time of writing, draft regulations had been published for comment but had not yet been finalized. Notice of Consultation, Call for comments on draft Electronic Commerce Protection Regulations (CRTC), (2011) C Gaz I, 2029; Industry Canada, Electronic Commerce Protection Regulations, (2011) C Gaz I, 2244.

“clearly and simply describe, in general terms, the function and purpose of the computer program that is to be installed if the consent is given.”

Much of the above would arguably be required under *PIPEDA*, though *PIPEDA* does not spell out the requirements with the same degree of detail. However, where *CASL* really gets interesting is in subsection 10(4); that subsection provides that, in addition to the above requirements, certain additional rules (described below) apply in respect of a request for consent to install a computer program that performs any of the following functions:

...that the person who seeks express consent knows and intends will cause the computer system to operate in a manner that is contrary to the reasonable expectations of the owner or an authorized user of the computer system:

(a) *collecting personal information stored on the computer system;*

(b) interfering with the owner’s or an authorized user’s control of the computer system;

(c) changing or interfering with settings, preferences or commands already installed or stored on the computer system without the knowledge of the owner or an authorized user of the computer system;

(d) changing or interfering with data that is stored on the computer system in a manner that obstructs, interrupts or interferes with lawful access to or use of that data by the owner or an authorized user of the computer system;

(e) causing the computer system to communicate with another computer system, or other device, without the authorization of the owner or an authorized user of the computer system;

(f) installing a computer program that may be activated by a third party without the knowledge of the owner or an authorized user of the computer system; and

(g) performing any other function specified in the regulations.²²²

Requests for consent to install programs that perform any of the above-listed or any prescribed functions must “clearly and prominently” and “separately and apart from the licence agreement”:

(a) describe the program’s material elements that perform the function or functions, including the nature and purpose of those elements and their reasonably foreseeable impact on the operation of the computer system; and

(b) bring those elements to the attention of the person from whom consent is being sought in the prescribed manner.²²³

Again, while it could be argued that *PIPEDA* may in certain circumstances require consent to be obtained in the above manner, *PIPEDA* does not include the level of detailed requirements that are included in *CASL*.²²⁴ The detailed requirements of *CASL* can be interpreted as a signal that Parliament is prepared to impose strict rules to regulate privacy when necessary, including in respect of the very kinds of activities activities (e.g. the use of DRM systems) that may implicate intellectual privacy as described herein. Along with components of some of the other privacy-protective legal models discussed in this part, this approach is considered further in

²²² *CASL*, *supra* note 220, s 10(5) [emphasis added].

²²³ *Ibid*, at s 10(4).

²²⁴ *CASL*, *supra* note 220.

Chapter 5 in connection with potential amendments to the *Copyright Act* to account for intellectual privacy.

III. What is Intellectual Privacy?

A. Defining Intellectual Privacy

At the outset of this dissertation, ‘intellectual privacy’ was characterized in general terms as “individuals’ freedom to access and enjoy creative works anonymously or in private.”²²⁵ That definition was purposefully general and focused on the particular context (i.e. copyright) with which this dissertation is concerned. However, as described in Part I of this chapter and as explored further below, intellectual privacy is certainly not restricted to the copyright context; far from it.²²⁶ In the passages below, this chapter asserts that no matter what is determined to be the full scope of intellectual privacy,²²⁷ it includes the copyright context and requires attention from copyright given the connection between intellectual privacy and creative endeavour, and given the important conflict (Chapter 3) and relationship (Chapter 4) between intellectual privacy and copyright.

Although the term “intellectual privacy” has been used in different contexts for at least 160 years (and probably longer)²²⁸, the concept

²²⁵ See *supra* note 3 and accompanying text.

²²⁶ See Part I of this chapter.

²²⁷ A discussion of the full scope of intellectual privacy is beyond the scope of this dissertation.

²²⁸ An exploration of the history of the usage of “intellectual privacy” is beyond the scope of this dissertation. Though hardly a rigorous or scientific investigation of the issue, a search of the term on Google Books, suggests that “intellectual privacy” has been used since at least as early as 1849. See *The Law Times*, vol 14, 1849 (“The strongest evidence that a man has retired in time from public affairs would be afforded by the fact that he had resolved to fall

appears to have only recently received any marked degree of attention in legal literature.²²⁹ One of the leading scholars in the area, Julie Cohen, has authored a series of seminal articles exploring intellectual privacy, including what she calls “the right to read anonymously.”²³⁰ Cohen defines intellectual privacy as follows:

[Intellectual privacy] concerns the extent of ‘breathing space,’ both metaphorical and physical, available for intellectual activity [and] extends both [a] to information about intellectual consumption and exploration and [b] to the physical and temporal

back upon domestic enjoyments and intellectual privacy...” at 337). This appears to be the earliest example of the term in any book available on Google Books. Consider also the following use of the term from a 1959 law review article: Morton L Price, “Billboard Regulation Along the Interstate Highway System” (1959-1960) 8 U Kan L Rev 88 at 88:

The right to be let alone can be cited as the essence of another vital interest which the general public has in the regulation of outdoor advertising. Improved techniques of communication have created an atmosphere in which it is extremely difficult to avoid the constant barrage of commercial propaganda. Recent revelations concerning motivational research and subliminal advertising have focused national attention on the problem of the dwindling sphere of ‘intellectual privacy’ [footnotes omitted].

²²⁹ Richards, *supra* note 16 at 408:

Although intellectual privacy has been recognized and protected in various areas of the law, it has received surprisingly little systematic attention in the legal literature. While its constituent parts have been examined here and there, we lack a broad theory of why and how we should protect privacy in intellectual explorations.

²³⁰ Key among her works that relate to intellectual privacy are Cohen, “DRM and Privacy”, *supra* note 3; Cohen, “A Right to Read Anonymously”, *supra* note 45.

circumstances of intellectual consumption within private spaces.²³¹

Other legal scholars have also proffered definitions of “intellectual privacy,” usually with reference to Cohen’s work.²³² For example, Peter Yu defines intellectual privacy as “the right to experience intellectual works in private, free from surveillance”²³³ and Neil Richards defines the term as “...the ability, whether protected by law or social circumstances, to develop ideas and beliefs away from the unwanted gaze or interference of others.”²³⁴ Richards in particular endeavours to posit a broad normative theory of “intellectual privacy,” drawing on the American legal experience in four areas where he suggests that intellectual privacy has been “protected and nurtured”: the freedom of thought and belief, spatial privacy, the right of intellectual exploration, and the confidentiality of communications.²³⁵ Building on his definition of “intellectual privacy”, he suggests that:

²³¹ Cohen, “DRM and Privacy”, *ibid* at 576. See also Cohen, “A Right to Read Anonymously”, *ibid* at 1003.

²³² See e.g. Gervais, “The Price of Social Norms”, *supra* note 49 at 64; Saif M Khan, “Copyright, Data Protection, and Privacy with Digital Rights Management and Trusted Systems: Negotiating a Compromise between Proprietors and Users” (2008-2009) 5 ISJLP 603 at 617:

Defining privacy is a prerequisite to fully exploring DRM's privacy-invasive implications. Most definitions incorporate at least one of two main components. First, intellectual privacy includes personal autonomy that guarantees ‘breathing space for thought, exploration, and personal growth.’ Second, intellectual privacy concerns spatial privacy that allows for intellectual consumption beyond public view. [footnotes omitted]

²³³ Yu, *Intellectual Property and Information Wealth*, *supra* note 98 at 338.

²³⁴ Richards, *supra* note 16 at 389. Anita Allen has characterized Richards’ “intellectual privacy” as a “complex hybrid”, being a “marriage of ‘associational’ and ‘informational’ privacy’”. See Anita Allen, *Unpopular Privacy: What Must We Hide?* (Cambridge: Oxford University Press, 2011) at 4.

²³⁵ Richards, *ibid* at 408.

...we should understand intellectual privacy as a series of nested protections, with the most private area of our thoughts at the center, and gradually expanding outward to encompass our reading, our communications, and our expressive dealings with others. At its core—the freedom of thought and belief—intellectual privacy should be all but absolute. As the interest expands to include other things and other people, however, some accommodation of competing interests must necessarily take place.²³⁶

Richards' theory is not without its critics,²³⁷ though it has been widely regarded as usefully contributing to the dialogue regarding intellectual privacy, particularly in respect of government encroachments on intellectual privacy. Richards' solution, however, sounds in large part similar to *PIPEDA* and other privacy laws—a plea not uncommon in American legal tradition where a privacy law of general application is lacking.²³⁸ In this dissertation, however, the limits of the *PIPEDA* model are tested and a more granular, copyright-specific solution is described.

Distilling the above articulations of intellectual privacy reveals first that the concept is about intellectual activity, or thinking.²³⁹ The

²³⁶ *Ibid.*

²³⁷ See e.g. Slobogin, *supra* note 110; Blitz, *supra* note 110.

²³⁸ Richards, *supra* note 16 at 431:

Protecting intellectual privacy in the digital age thus requires a twopronged strategy. First Amendment doctrine can be used to directly restrain government actions that threaten intellectual privacy. But constitutional doctrine has its limits. Because many threats to intellectual privacy lie beyond the reach of constitutional doctrine, we must also seek to encode protections into our statutory laws and the very fabric of our social norms and institutions.

²³⁹ The Merriam Webster online dictionary defines “intellectual” as including: 1(a) of or relating to the intellect or its use (b) developed or chiefly guided by the intellect rather than by emotion or experience: rational (c): requiring use of

particular elements of that activity include accessing, receiving, processing and enjoying information (what Cohen calls “consumption”), as well as the related process of forming and developing ideas and beliefs (what Cohen calls “exploration”). These activities are common to all people and are not reserved to great minds or creators. In the course of or in relation to both consumption and exploration, it is also important to note that individuals may put pen to paper, fingers to keyboard, or voice to speech recognition software, with a view to furthering their thought (i.e. jotting down notes or ideas) or to creating a new work of their own. Unpublished writings are thus closely linked to the intellectual and creative activities with which this dissertation is concerned.²⁴⁰

The “privacy” in “intellectual privacy” connotes that the intellectual activity described above is performed under conditions that protect against exposure to others without the knowledge and consent of the thinker. Accordingly, the activity must not be subject to surveillance or observation by others; others must be unable to access information about the activity before, during or after it takes place.

the intellect; 2(a): given to study, reflection, and speculation (b) engaged in activity requiring the creative use of the intellect” and “intellect” as including “1(a) the power of knowing as distinguished from the power to feel and to will: the capacity for knowledge (b) the capacity for rational or intelligent thought especially when highly developed.” Merriam Webster Online Dictionary, *sub verbo* “intellectual” & “intellect”.

²⁴⁰ See generally Neil Richards, “Brandeis, Privacy and Speech” (2010) 63 Vand L Rev 1295 at 1347 [Richards, “Brandeis”]:

Intellectual privacy can be threatened in a number of ways, but one of the most important is through the disclosure or surveillance of records relating to reading, thinking, and *non-public writing*. In the past, such records have included letters, diaries, library records, and transcripts of phone conversations [emphasis added].

The above descriptions of intellectual privacy also reveal that “intellectual privacy” is a state which can be achieved in a number of different ways, including in some cases through informational or spatial privacy or, put more generally, by (metaphorically) removing oneself from people, places, circumstances or influences which do not permit one to engage freely in intellectual activity.²⁴¹ Spatial privacy has always been and continues to be a primary source of enabling intellectual privacy; this is not surprising because intellectual privacy involves activities which are often undertaken in private spaces, particularly in the home.²⁴² To take another example (which does not fit neatly in any traditional category of privacy), the ability to speak, read or write a foreign language can provide a means of achieving intellectual privacy by removing one’s intellectual activities and communications from others: “... the ability [of slaves] to speak languages that owners could not understand sustained ethnic and tribal identities and permitted some intellectual privacy.”²⁴³ Different forms of social institutions, conventions and practices can also facilitate intellectual privacy, including libraries.²⁴⁴

Since removing oneself from others can sometimes be with the aim of achieving solitude for thought and sometimes with the aim of exposing one’s intellectual activities to other people, places or influences (including those which are thought to be *conducive* to intellectual activity), intellectual privacy is therefore also about the

²⁴¹ See *supra* note 95 and accompanying text.

²⁴² See generally Cohen, “DRM and Privacy”, *supra* note 3.

²⁴³ See e.g. Linda K Kerber, “The Revolutionary Generation: Ideology, Politics and Culture in the Early Republic” in Eric Foner, ed, *The New American History* (Philadelphia: Temple University Press, 1997) at 44. Similarly, reading books in a foreign language or writing notes in a foreign language may help “remove” such intellectual activities from others.

²⁴⁴ See ALA, “Interpretation of the Library Bill of Rights”, *supra* note 108; Richards, *supra* note 16 at 419-21.

ability to choose and to control what consumption and exploration activities, if any, are revealed and to whom.²⁴⁵

It should also be noted that the above passages describe the intellectual privacy in terms of a state of being as opposed to a legal right *per se*. In order to achieve that state, however, it is necessary in many cases that there is a legal right to it. In other words, while social norms and circumstances may often facilitate or be sufficient for individuals to achieve a measure of intellectual privacy, there are a variety of circumstances, including in relation to many forms of consumption of copyright works, where a legal rule is necessary to achieve a state of intellectual privacy. For example, given the prevalence of business practices and incentives to diminish intellectual privacy as described in Chapter 3 (and the lack of an effective or practical means in many cases to avoid such diminishment), it appears necessary that there be a legal protection(s) in place to facilitate and protect individuals' intellectual privacy in connection with copyright works. Indeed, because of the close connection between intellectual privacy, freedom of thought and freedom of expression, a number of scholars have argued in favour of a *constitutionally*-protected legal right to intellectual privacy.²⁴⁶

It is hoped that the foregoing introduction to intellectual privacy is uncontroversial. While subjective and cultural conceptions of

²⁴⁵ See e.g. William Howard Adams, *The Paris Years of Thomas Jefferson* (New Haven: Yale University Press, 2000) at 109.

²⁴⁶ See e.g. Cohen, "A Right to Read Anonymously", *supra* note 45 ("[R]eading is so intimately connected with speech and freedom of thought that the First Amendment should be understood to guarantee such a right" at 983). See also *Convention for the Protection of Human Rights and Fundamental Freedoms*, 4 November 1950, 213 UNTS 221 at 223, Eur TS 5, art 10, which provides as follows: "Everyone has the right to freedom of expression. This right shall include freedom to hold opinions and to receive and impart information and ideas without interference by public authority and regardless of frontiers" [emphasis added].

privacy vary, intellectual privacy seems to be functionally important to intellectual activity—the latter often requires conditions of privacy in relation to the consumption and exploration activities described above. The remaining sections of this part reinforce the concepts above and further highlight some of values that are interrelated with intellectual privacy. Section B of this part briefly reinforces the widely-held notion that intellectual consumption and exploration can be revealing of an individual's thoughts. Building on that basic premise, Section C underscores the values that are interrelated with intellectual privacy, including autonomy, identity, and expression (with special emphasis on creative endeavour).²⁴⁷

²⁴⁷ The terms “freedom of expression” and “creative endeavour” are used somewhat interchangeably in the sections that follow. The former phrase is customarily used in the context of the *Charter* and is the near-equivalent of the American concept of “freedom of speech.” The latter phrase is intended to refer to a similar sort of expressive activity but with a particular bent toward the kinds of expression that are encouraged and protected by copyright. Indeed, in the United States the latter has been said to have a “constitutional dimension” in so far as authors have the right to control the public distribution creative of work: see Cohen, “A Right to Read Anonymously”, *supra* note 45 at 1003:

In *Harper & Row, Publishers, Inc. v. Nation Enterprises*, which involved the unauthorized release of excerpts from a soon-to-be-published book, the Court made clear that its refusal to invoke the fair use doctrine was motivated in part by concern for the author's First Amendment rights. The Court observed that the Framers of the Constitution ‘intended copyright itself to be the engine of free expression.’ It reasoned that copyright policies reserving control over distribution to the author serve First Amendment as well as copyright purposes. In particular, authors enjoy the same right not to speak accorded other speakers. Copyright protects this right by securing to authors a right of creative control -- a right not to publish ideas before they have been developed and polished to the author's satisfaction.

B. Reading, Writing and Thought

The URLs which people use reveal a huge amount about their lives, loves, hates, and fears. [...] People use the web in crisis, when wondering whether they have STDs, or cancer, when wondering whether they are homosexual and whether to talk about it, to discuss political views [...] The act of reading, like the act of writing, is a pure, fundamental, human act. It must be available without interference or spying.

- Sir Tim Berners-Lee²⁴⁸

The study of an individual's intellectual consumption is believed by many to provide a window to an individual's thoughts²⁴⁹—it can be made to “speak volumes.”²⁵⁰ Commentators frequently study

²⁴⁸ Sir Tim Berners-Lee, “No Snooping” (9 March 2009), online: World Wide Web Consortium <<http://www.w3.org/DesignIssues/NoSnooping.html>>.

²⁴⁹ See e.g. Richards, *supra* note 16 at 389:

[A]s we have come to rely on computers and other electronic technologies to live our personal and professional lives, a vast amount of information about our activities is recorded, logged, and made available for access by others. This has become increasingly true as we use these technologies not just to shop, but to think, read, and communicate. The information created by these processes includes not only our preferences in toothpaste, but our tastes in politics, literature, religion, and sex. We are creating, in other words, a record of our intellectual activities—a close proxy for our thoughts—in unprecedented ways and to an unprecedented degree.

²⁵⁰ This is precisely why businesses and others collect such information for marketing and other purposes. Cohen, “A Right to Read Anonymously”, *supra* note 45 at 981:

In truth, however, the new information age is turning out to be as much an age of information about readers as an age of information for readers. ... In the new age of digitally transmitted information, the simple, formerly anonymous acts of reading, listening, and viewing — scanning an advertisement or

the libraries of great minds and public figures in search of insight into their thinking, as well as who they are or were.²⁵¹ President Obama's book list is said to have "shaped a president."²⁵² Courts in the United States in criminal proceedings and sentencing hearings often admit evidence about what music an accused listened to or whether they watched, for example, *Natural Born Killers* or other films.²⁵³ Such evidence is admitted because, *inter alia*, it is thought

a short news item, browsing through an online novel or a collection of video clips — can be made to speak volumes, including, quite possibly, information that the reader would prefer not to share.

See also Gervais, "The Price of Social Norms", *supra* note 49 ("Many users will also have another paramount concern: intellectual privacy. By determining what a person reads, listens to, and exchanges, much can be learned about one's personality and preferences" at 64).

²⁵¹ See e.g. Yvan Lamonde & Andrea Rotundo, "Entering Personal Libraries" in Yvan Lamonde, Patricia Lockhart Fleming & Fiona A Black, eds, *History of the Book in Canada, vol 2, 1840-1918* (Toronto: University of Toronto Press, 2004) ("Analysis of a person's library can suggest his or her intellectual evolution..." at 243); Francine du Plessix Gray, *At Home with the Marquis de Sade* (New York: Penguin, 1998) (describing the reading habits of the young Marquis de Sade, including the books in his uncle's personal library and the hundreds of books that Sade himself assembled during his time in Vincennes and the Bastille at 26-27, Chapter XXI).

²⁵² Michiko Kakutani, "From Books, New President Found Voice" *New York Times* (18 January 2009), online: *New York Times* <<http://www.nytimes.com/2009/01/19/books/19read.html>>.

²⁵³ See e.g. Helen A Anderson, "The Freedom to Speak and the Freedom to Listen: The Admissibility of the Criminal Defendant's Taste in Entertainment" (2004) 83 Or L Rev 899 at 900:

Evidence that the defendant viewed the movie *Natural Born Killers* has been introduced in a number of murder trials. In these and other criminal cases, courts have allowed evidence of the defendant's viewing or listening habits to show motive, intent, state of mind, or to support an aggravating factor at sentencing. In such cases the Constitution is rarely mentioned, even though the First Amendment has been held to protect consumers as well as the producers of First Amendment speech.

by some to be probative of the accused's motive, intent or state of mind.²⁵⁴

Where an individual's liberty is at stake, however, evidence about an individual's access to and enjoyment of copyright works is not universally accepted as being probative of their state of mind.²⁵⁵ For example, in one American case where a jury was shown *Natural Born Killers*—a movie which the majority of the Georgia Supreme Court ruled showed “[the accused's] bent of mind”²⁵⁶—a dissenting judge criticized the majority's rationale for showing the movie to the jury:

Based on this broad reasoning, any book, movie, record, or television program that includes a crime similar to the one with which an accused is charged would be relevant to show that individual's bent toward criminal activity. Under this expansive test, reading the works of Nobel Prize winning authors like Toni Morrison and William Faulkner can become evidence that an accused had a “bent of mind” to commit murder.²⁵⁷

Similarly, Canadian courts have sometimes refused to admit evidence of an accused's reading habits on the basis that the evidence has little probative value in showing thoughts or a state of

And, while courts reject a causal link between art and crime when artists or the entertainment industry are civil defendants, the assumption of causation seems to underlie the admission of viewing, reading, or listening habits in criminal cases.

²⁵⁴ *Ibid.*

²⁵⁵ *Ibid.*

²⁵⁶ *Beasley v State* 502 SE2d 235 at 238 (Ga 1998).

²⁵⁷ *Ibid* at 244, where the dissenting judge goes on to add: “Because this rationale is simplistic and overreaching, I find it unpersuasive as a basis for allowing the jury to view the movie.” Incidentally, Toni Morrison's *Song of Solomon* is reported as among President Obama's favourite reading material. See Kakutani, *supra* note 252.

mind and is prejudicial. For example, in *R v Bernardo*,²⁵⁸ an Ontario court refused to admit into evidence a series of newspaper articles on crimes of violence that were seized in the home of the accused. Remarking that the newspaper articles “indicate an interest or fascination with violence”, the court refused to admit the evidence on the basis that it had little or no probative value.²⁵⁹ Although some other articles and flyers were ruled admissible on other grounds, the court also refused to admit the novel *American Psycho* absent specific evidence to support the Crown’s position that the novel was a “blueprint” for the crime at issue.²⁶⁰

On the other hand, as further evidence of the widely-held belief that evidence of a person’s intellectual habits can be probative of their thoughts or propensities,²⁶¹ Canadian courts have admitted

²⁵⁸ *R v Bernardo* [Evidence - Articles Seized in Home] [1995] OJ No 1394.

²⁵⁹ *Ibid* at para 3.

²⁶⁰ *Ibid* at para 18:

Exhibit F is a novel "American Psycho". Exhibit F2 is the receipt indicating that novel was purchased on the 17th April 1991. Exhibit F3 is a book review in the Toronto Sun which states, in part, "American Psycho is Sicko". The Crown seeks to introduce this book because it was purchased two months before Leslie Mahaffy was kidnapped and, according to their submissions, is a blueprint or a pattern for her kidnapping, rape and murder. I have read the summary prepared by the Crown, but have not read the novel itself. There is no question that what is written in this novel is violent, perverted and to use the vernacular 'sick'. This book, if tendered and read in whole or in part by the jury, would have significant prejudicial effect. Its probity is, in my opinion, tentative. I am not prepared, in the absence of some specific evidence from a witness that this book was used as a "blueprint" or as a model for the kidnapping, rape and killing of Ms. Mahaffy or Ms. French, to rule it admissible. Subject to the unfolding of events through viva voce evidence this Exhibit is not admissible.

²⁶¹ I am indebted to Jane Bailey for pointing out that this idea seems also to be present in the context of *Charter* decisions relating to freedom of expression

evidence of an individual's reading materials where the accused wishes to introduce the evidence to show another individual's state of mind (e.g. to support a provocation defence).²⁶²

What emerges from such cases is both a doubt about the ability of intellectual consumption to show thought—because reading about fertilizer might indicate that a person is an avid gardener, a chemist, a historian or interested in making a home-made bomb, among other possibilities—and a recognition that such consumption may, particularly when combined with other information, be highly probative of thought. The latter point is of particular importance in the information age where vast quantities of isolated bits of information about intellectual consumption can be combined with one another ostensibly to provide an unprecedented window into an individual's thinking.²⁶³

Consistent with the notion that information about intellectual *consumption* can provide insight into thought, an individual's

and obscenity and child pornography. See e.g. *R v Sharpe*, 2001 SCC 2 (holding that restrictions on private possession of child pornography must be narrowed on constitutional grounds at paras 25, 26, 75, 105-110).

²⁶² Prejudice to the Crown is not a ground for refusing to admit such evidence. See e.g. *R v Valley*, 1986 CanLII 110 (ON CA) at paras 54-56:

In my opinion, the magazines were linked to the deceased, they were relevant on the issue of provocation, and ought to have been admitted in evidence. I am unable to say that a jury might not conclude that the magazines were evidence of a propensity on the part of the deceased, that could support the appellant's testimony that the deceased indecently assaulted him, having regard to the fact that the deceased was nude, was wearing the device previously described and the appellant was clothed. Although the judge has a discretion to exclude evidence proffered by the prosecution if the evidence is of slight probative value and gravely prejudicial, no discretion exists to exclude relevant evidence offered by an accused on the ground that it is prejudicial to the Crown: see *R v Hawke* (1975), 22 CCC (2d) 19.

²⁶³ See e.g. Berners-Lee, *supra* note 248; Richards, *supra* note 16.

expression and writings are also thought to provide such insight. With the act of publication, authors (in the broadest sense of that term) relinquish that part of their intellectual privacy which is reflected in or revealed by the published work.²⁶⁴ Thought is also reflected in unpublished writings, the seizure of which has been considered to be a gross invasion of intellectual privacy, akin to reading a person's thoughts or illegally extracting oral statements.²⁶⁵ In 1763, John Wilkes sued the King's sheriffs for breaking into his home, reviewing his papers and taking his diary

²⁶⁴ See e.g. W Arthur, "Notable Men of Wales: George Herbert" in Charles Wilkins, ed, *The Red Dragon: The National Magazine of Wales Volume VII, January to June 1885* (Cardiff: Daniel Owen and Company, 1885) at 385-86:

It is not merely that our outward impressions of an author are definite; we creep into his mind and explore its inmost recesses. The man has infused himself into his book; it is a transcript from his brain, plain for all to read. He gains our interest, our sympathy, but obviously it is only at the price of his own intellectual privacy.

²⁶⁵ Lord Temple, "A Letter to the Right Honourable the Earls of Egremont and Halifax, His Majesty's Principal Secretaries of State, on the seizure of papers" (19 May 1763) in John Almon, ed, *Biographical, literary, and political anecdotes, of several of the most eminent persons of the present age* (London: T.N. Longman, and L.B. Seeley, 1797) at 187-88. See also Father of Candor, "A Letter Concerning Libels, Warrants, the Seizure of Papers" in *The Gentleman's and London magazine: or monthly chronologer, 1741-1794* (January 1765) at 43:

The laws of England are to tender to every man accused, even of capital crimes, that they do not permit him to be put to torture to extort a confession, nor oblige him to answer a question that will tend to accuse himself. How then can it be supposed, that... any common fellows under a general warrant... [may] seize and carry off all his papers; and then at his trial produce these papers... in evidence against himself... This would be making a man give evidence against and accuse himself, with a vengeance. And this is to be endured, because the prosecutor wants other sufficient proof, and might be traduced for acting groundlessly, if he could not get it; and because he does it truly for the sake of collecting evidence.

and letters. A letter supporting Wilkes put the point eloquently as follows:

[a] man's writings lying in his closet, not published, are no more than his thoughts, hardly brought forth even in his own account, and, to all the rest of the world, the same as if they yet remained in embryo in his breast. [...] The rack itself is hardly a more inhuman mode of accusation, or tyrannical method of proof. Both are equally against the first laws of nature; and nothing can be more unlike the benign spirit of our happy constitution.²⁶⁶

Consider also the case of Sir Thomas Browne's famous *Religio Medici* which was written for the author's "private exercise and satisfaction."²⁶⁷ A copy of this book was "most imperfectly and surreptitiously"²⁶⁸ published without Browne's knowledge or consent, leading him to rectify aspects of the work and to subsequently publish a "full and intended"²⁶⁹ copy of it, along with an unusual note "To the Reader" in which he explains the events just described. Being more mature at the time of publication than when he wrote the work, Browne explains that what he "set down many years past" might not be agreeable to his present self.²⁷⁰ His

²⁶⁶ Lord Temple, *ibid.*

²⁶⁷ JA Symonds, ed, *Sir Thomas Browne's Religio medici, Urn burial, Christian morals, and other essays* (London: W Scott, 1886) at 6.

²⁶⁸ *Ibid.*

²⁶⁹ *Ibid.*

²⁷⁰ *Ibid.* It is interesting to note that in the same "To the Reader" at 6, Browne highlights the value that access to books can have in the writing process:

[Religio Medici] was penned in such a place, and with such disadvantage, that (I protest), from the first setting of pen unto paper, I had not the assistance of any good book, whereby to promote my invention or relieve my memory, and therefore there might be real lapses therein, which others might take notice of, and more than I suspected myself.

“To the Reader” has been characterized by one Browne scholar as “the voice of violated personal and intellectual privacy...”²⁷¹ The temporal discussion of the violation is important to consider in the context of records of individual’s intellectual activities in the information age. For example, the works that one chooses to search for and enjoy as a teenager, not only do not likely provide an accurate picture of one’s adult thoughts but also may be a more grievous invasion of the intellectual privacy of the adult person who may have distanced their thoughts and views from those of their teenage self. An absence of intellectual privacy can thereby threaten individuals’ ability to grow, change and mature.²⁷² Concerns such as these motivate contemporary academic and policy discourse regarding a potential “right to be forgotten.”²⁷³

²⁷¹ Claire Preston, *Thomas Browne and the Writing of Early Modern Science* (Cambridge: Cambridge University Press, 2005) at 14:

It is – perhaps bathetically and hyperbolically – Browne’s privacy which has been insulted by the illicit publication of *Religio Medici*. This small but piercing injury prompts the extreme reconfiguration of the apocalypse as, for the only time in his career, social chaos, as the kind of fundamental incivility which, in earlier instalments of human history, founders states and families, in which uncivil assaults on individuals are obviated only by the divine imposition of a legally based civil society. As he explains in the preface, his notion of social order and hierarchy, represented in King and parliament, is being catastrophically eroded by civil affronts from the press, so that even his own injury – a rude, helpless exposure to the general view – is owing to the same foundered properties. With this uncharacteristically dismal vision of the apocalypse, Browne seems to suggest that his personal misadventure with the press is a microcosmic signature of the end of days...

²⁷² See Remarks of Jennifer Stoddart, Privacy Commissioner of Canada, June 6, 2011, online: CBC <<http://www.cbc.ca/spark/2011/06/full-interview-jennifer-stoddart-on-online-privacy/>>. See also Part I of this chapter.

²⁷³ See generally Viktor Mayer-Schönberger, *Delete: The Virtue of Forgetting in the Digital Age*, (Princeton: Princeton University Press, 2009); Rolf H Weber, “The Right to Be Forgotten: More Than a Pandora’s Box?” (2011) 2 JIPITEC 120.

The simple premise underlying each of the above examples is that an individual's intellectual activities are widely believed to reveal something about an individual's thinking in many circumstances. Based on the above, it may be obvious for some why intellectual privacy is important and deserving of legal protection. However, to help bolster our definition of intellectual privacy and the reasons why it should be protected, the remaining sections of this chapter explore some of the widely-held values that are interrelated with intellectual privacy and the harms that can flow from its absence.

C. Values that are interrelated with Intellectual Privacy

Given the basic premise discussed in the preceding section of this chapter, it should come as no surprise that freedom of thought and related values of autonomy, identity and expression are among the values that are interrelated with intellectual privacy. Indeed, privacy in general is widely recognized as being essential to individuals' freedom of thought, autonomy and the development of identity.²⁷⁴ The *Charter* jurisprudence described earlier in this

²⁷⁴ See e.g. *R v Bengert* (No 8) [1979] BCJ No 1709 (SC) at para 5:

With the advance of technology, the possibilities for the infringement of privacy have proliferated. The legislation is designed to prevent anyone, including law enforcement authorities, abusing the opportunities that technology now offers for intercepting private communications. I think its passage reflects Parliament's concern that legal sanctions should be available to minimize infringements on the right of privacy, a right which is essential to freedom of thought and freedom of speech.

The preamble to *The Australian Privacy Charter* also draws the connection:

A free and democratic society requires respect for the autonomy of individuals, and limits on the power of both state and private organizations to intrude on that autonomy... privacy is a key value which underpins human dignity and other key values such as freedom of association and freedom of speech...

chapter is consistent with this view²⁷⁵, recognizing, among other things, that because “freedom from state intrusion and conformist social pressures is integral to individual flourishing and diversity, [...] ‘privacy is at the heart of liberty in a modern state’”²⁷⁶ and that:

[the *Charter*], raises to the highest level by calling “a fundamental freedom” the freedom of thought, belief, opinion and expression, including freedom of the press and other media communication. What could be more implicit in freedom of thought, belief, opinion and expression than the right to hold those beliefs and communicate those opinions privately? [...] It is only through the exercise of our privacy rights that we are able to distinguish ourselves from animals. It is only on that philosophical plane that we are truly distinct from other societies and cultures that are either dictatorships

Australian Privacy Charter Council (APCC), *Australian Privacy Charter* (December 1994), online: APCC <<http://www.privacy.org.au/apcc/>>. For an American example, see *benShalom v Secretary of Army*, 489 FSupp 964, 976 (EDWis1980) (“The ‘...autonomous control over the development and expression of one’s intellect, interests, tastes, and personality’ are among the most precious of rights protected by the First Amendment. *Doe v Bolton*, 410 US 179, 211, 93 SCt 739, 757, 35 LEd2d 201 (1973) (Douglas, J., concurring)” at 974).

²⁷⁵ See e.g. *Ontario (Attorney-General) v Dieleman*, *supra* note 158 at para 548:

the ‘flip side’ of a constitutional concern for privacy is the protection of personal autonomy. In this respect, Sopinka J., in *Rodriguez v British Columbia (Attorney-General)* 1993 CanLII 75 (SCC), (1993), 107 DLR (4th) 342, 85 CCC (3d) 15, [1993] 3 SCR 519, described the section 7 interest in a woman’s decision to abort at 391: ‘In my view, then, the judgments of this court in *Morgentaler* can be seen to encompass a notion of personal autonomy involving, at the very least, control over one’s bodily integrity free from state interference and freedom of state-imposed psychological and emotional stress.’

See also *R v O’Connor*, *supra* note 129 at para 111.

²⁷⁶ *R v Sharpe*, *supra* note 261 at para 26.

or socially constrained cultures. It is of the highest moment that we preserve the rights to our privacy.²⁷⁷

Privacy in respect of intellectual activity in particular is where the values of autonomy and identity take on special importance.²⁷⁸ Accessing and enjoying creative works are among the essential ways that individuals self-reflect and develop their identity, helping them to determine “who one wants to be, what one wants to believe, and with whom one wants to associate”²⁷⁹:

...what makes privacy distinctive is its direct support of the moral and ethical nature of human beings as self-directed, autonomous beings... [...] Autonomy, the

²⁷⁷ *R v Watts*, [2000] BCJ No 2721 (BC Prov Ct.) (followed in a civil proceeding arising from the same facts: *Watts v Klaemt* [2007] BCJ No 980).

²⁷⁸ Cohen, “DRM and Privacy”, *supra* note 3 at 582:

Some philosophers argue that where certain deeply personal activities are concerned, privacy denotes not only a condition of (relative) inaccessibility, but also a zone of noninterference with individual choice. The usual examples relate to rights to control one's own person (e.g., decisions about reproduction, or about intimate relationships), but one might extend the argument to encompass rights to control one's own intellectual development [footnotes omitted].

²⁷⁹ Julie Cohen, “Intellectual Privacy and Censorship of the Internet” (1997-1998) Seton Hall Const LJ 693 (“What I have talked about is a process of constructing the self. Reading and listening and viewing help determine who one wants to be, what one wants to believe, and with whom one wants to associate” at 697). See also Ray Erwin Baber, *Marriage and the Family* (New York: McGraw Hill, 1953) at 202, 259-260 (discussing the importance of intellectual privacy to the development of children's ideas, relationships and identity); David Matheson, “Overprotection, Surveillance, and the Development of Virtue” (27 February 2006), online: On the Identity Trail <<http://www.idtrail.org/files/Matheson%20-%20Overprotection....pdf>>. Consider also that the *Declaration of the Principles of International Cultural Co-operation*, UNESCO, (1966) at art VII.1 states that “[b]road dissemination of ideas and knowledge, based on the freest exchange and discussion, is essential to creative activity, the pursuit of truth and development of the personality.”

ability to choose freely, is key to (informational privacy, decisional privacy and accessibility privacy) and, thus, important to readers in allowing them to choose how and what to read but also how what they read helps them make themselves.²⁸⁰

It is also significant for the purposes of this dissertation that the values of autonomy and free thought are intimately intertwined both with intellectual privacy and also with values of freedom of expression and creative endeavour.²⁸¹ In *Solitude: A Return to the*

²⁸⁰ William Aspray & Philip Doty, *Privacy in America: Interdisciplinary Perspectives* (Plymouth: Scarecrow Press, 2011) at 213, which also includes the following statement: "Reading is one important way in which people reflect about who they are and try our identity in a number of ways and is linked to the protection of intellectual privacy." These values are also recognized and reinforced by libraries: ALA, "Privacy: An Interpretation of the Library Bill of Rights", *supra* note 108. See also Waldo, Lin & Millett, *supra* note 22 at 236:

Unlike some who see privacy as a right or a good in and of itself, the library community sees privacy as a necessary condition for the accomplishment of its primary goal, which is to provide the atmosphere and the resources for patrons to educate themselves in whatever way they desire.

²⁸¹ For an example of one of the different ways that intellectual privacy and expression can be intertwined, consider the following passage from *R v Sharpe*, *supra* note 261 at para 26: "Privacy may... enhance freedom of expression claims under s. 2(b) of the *Charter*... in part because the freedoms of conscience, thought and belief are particularly engaged in the private setting", citing *Canada (Human Rights Commission) v Taylor*, [1990] 3 SCR 892. In other words, it can be argued that where a particular form of expression might be considered offensive (e.g. hate literature) if it were published, the court must take into account the unpublished nature of the work and thus give particular consideration to the individuals' strong claims to freedom of thought and belief. See also *Stanley v Georgia*, (1969) 394 US 557 at 558 ("These are the rights that appellant is asserting in the case before us. He is asserting the right to read or observe what he pleases -- the right to satisfy his intellectual and emotional needs in the privacy of his own home. He is asserting the right to be free from state inquiry into the contents of his library"). One commentator studying the early social history of the term "privacy", including in literature, identifies one poet's conception of privacy as "inherently conducive to mental

Self,²⁸² acclaimed psychiatrist and author Anthony Storr conducts a comprehensive exploration of the relationship between creativity and solitude. Using the lives of a number of well-known writers, scholars, philosophers, scientists and composers as examples, Storr posits that the capacity to be alone is “linked with self-discovery and self-realization; with becoming aware of one’s deepest needs, feelings, and impulses” and that “...creative attitude and the ability to have peak experiences depends upon being free of other people; free, especially, from neurotic involvements, from ‘historical hangovers from childhood,’ but also free of obligations, duties, fears, and hopes.”²⁸³ For Storr, it is during these times of solitude that individuals are likely to engage in creative endeavors that play an important role in “defining individual identity and in giving meaning to a person’s life.”²⁸⁴

Indeed, creators themselves often cite the need for intellectual privacy.²⁸⁵ Sometimes closely related to concerns about censorship, attacks on intellectual privacy can be simultaneously understood as attacks on artistic liberty. In January 1535, French officers seized the books and papers of the poet Marot at his home in Blois. Marot complained to the King as follows:

O sacrilegious judge, who gave you the legal right or
privilege to go tampering and wrecking in the cabinet

tranquility and creativity”. See Ronald Huebert, “Privacy: The Early Social History of a Word” (1997) 105 *Sewanee Review* 21 (commenting on Marvell’s poem “The Garden”).

²⁸² Anthony Storr, *Solitude: A Return to the Self* (New York: Ballentine, 1988) at 21.

²⁸³ *Ibid.*

²⁸⁴ *Ibid* at 73.

²⁸⁵ See e.g. Virginia Woolf, *A Room of One’s Own* (London: Hogarth Press, 1929) (suggesting that spatial privacy is a part of what is necessary in order to write: “[a] woman must have money and a room of her own if she is to write fiction...” at 4). Thanks to Jane Bailey for raising the important question of whether this quote in particular may reveal more about inequality than it does about creativity.

of the sacred Muses? It is true that they found forbidden books there; but that is no offence in a poet, who should be allowed a long rein, and have nothing hidden from him, whether it be magic, necromancy or cabalism; there is no doctrine, written or spoken, that a true poet should not understand in order to do his duty as a writer.²⁸⁶

The cabinet of the sacred Muses has been called a symbol of intellectual privacy and artistic liberty.²⁸⁷ As Marot's experience suggests, the very nature of creative endeavour requires that individuals have access to all manner of creative works without fear that they may be discovered or interfered with by the King.²⁸⁸ The objective of that access, however, is undermined when it cannot be achieved under conditions of intellectual privacy. The effect of providing access without intellectual privacy in many cases may be tantamount to censorship—i.e. individuals often *self-*

²⁸⁶ Annabel Patterson, "Re-opening the Green Cabinet: Clement Marot and Edmund Spenser" in Arthur F Kinney, Dan S Collins, eds, *Renaissance Historicism: Selections from English Literary Renaissance* (Amherst: University of Massachusetts Press, 1987) at 73.

²⁸⁷ For a discussion of how Marot's poem simultaneously reflects "the right of the individual to privacy and the responsibility of poets to wade into dangerous waters; hence their special or privileged status in society," see Annabel M Patterson, *Censorship and Interpretation: The Conditions of Writing and Reading in Early Modern England* (Madison: University of Wisconsin Press, 1991) at 6.

²⁸⁸ See also John Milton, "Areopagitica: A Speech for the Liberty of Unlicensed Printing, to the Parliament of England" in *The Prose Works of John Milton* (London: Westley and Davis, 1835) at 108:

Since therefore the knowledge and survey of vice is in this world so necessary to the constituting of human virtue, and the scanning of error to the confirmation of truth, how can we more safely, and with less danger, scout into the regions of sin and falsity than by reading all manner of tractates and hearing all manner of reason? And this is the benefit which may be had of books promiscuously read.

censor their activities as a result of a lack of intellectual privacy.²⁸⁹ Had he known that the King was watching what books he read, Marot might not have accessed many books; he might as well have been prohibited from accessing the works by way of censorship. The curious reader might ask what steps Marot may have taken following the raid described above, in order to prevent his future intellectual activities and books from coming to the attention or into the possession of the authorities. As one contemporary author elegantly puts the issue: “[s]urveillance is inimical to creativity. We cannot expect people to ‘stand on the shoulders of giants’ to create in the full glare of spotlights.”²⁹⁰

Indeed, surveillance (in the broadest sense of that term) undermines the diversity and richness of creative endeavour, “stunting” our creativity.²⁹¹ The knowledge that one’s intellectual

²⁸⁹ It should be noted that this effect is relevant to and important for all people, not just creators and not only in connection with creative endeavour.

²⁹⁰ Greenleaf, “IP, Phone Home”, *supra* note 48. In the same work, Greenleaf notes that “[r]esearchers (or lawyers) do not want anyone to know what digital works they are consulting. An author wanting permission to include an extract in an anthology or other collection does not want her publishing plans indirectly disclosed to rival publishers.” *C.f.* Jane Bailey, “Life in the Fish Bowl: Feminist Interrogations of Webcamming” in Kerr, Steeves & Lucock, *supra* note 1, citing Hille Koskela, “Webcams, TV Shows and Mobile phones: Empowering Exhibitionism” (2004) 2 *Surveillance & Society* 199 at 199:

To be (more) seen is not always to be less powerful. By rebelling against the shame embedded in the conception of the private, people refuse to be humble. They may gain power, but it does not head for control over others but, rather, blur and mix the lines of control. Televisualisation, cyberspace presentation, and mobile phone counter observation also raise new questions considering 'traditional' surveillance. Images can be played with, and can work as a form of resistance. Sometimes it is more radical to reveal than to hide.

²⁹¹ OPC, “The Privacy Implications of Deep Packet Inspection”, online: OPC <http://dpi.priv.gc.ca/index.php/essays/the-privacy-implications-of-deep-packet-inspection/#_ftn8> (“[I]f [deep packet inspection] becomes a fact of life,

activities may be observed by others, including by means of surveillance, often impacts on one's behaviours. That much we know from Foucault's panopticon²⁹² and Orwell's *Nineteen Eighty Four*,²⁹³ among many others.²⁹⁴ Such observation can affect choices

informed consumers may curtail their online communications rather than risk its release to others. This would stunt our creativity and intellectual privacy, so critical to the development of our ideas and free speech.")

²⁹² Michel Foucault, *Discipline and Punish: The Birth of the Prison*, 2d ed, translated by Alan Sheridan (New York: Vintage Books, 1995) at 224.

²⁹³ George Orwell, *Nineteen Eighty-Four* (London: Secker and Warburg, 1949) at 4-5:

There was of course no way of knowing whether you were being watched at any given moment. [...] It was even conceivable that they watched everybody all the time. [...] You have to live - did live, from habit that became instinct - in the assumption that every sound you made was overheard, and, except in darkness, every movement scrutinized.

²⁹⁴ Although it is not a theme advanced in this dissertation, surveillance initiatives, including in the copyright context can be understood as an attempt to exercise power over the targets of the surveillance. See Foucault, *supra* note 292 (Foucault notes that power is increased with the increases in knowledge: "knowledge follows the advances of power, discovering new objects of knowledge over all the surfaces on which power is exercised" and "the formation of knowledge and the increase of power regularly reinforce one another in a circular process" at 224. Foucault talks about the ability of the Panopticon to act as a "laboratory" to alter behaviour in people at 203-204. In his discussion of panopticism generally, Foucault also points out that while contract may underwrite the acceptance of discipline in society, panopticism is "the technique, universally widespread, of coercion" at 222. This language could equally describe a number of the themes developed by Cohen and discussed in this dissertation. In Cohen, "Examined Lives", *supra* note 13 at 1408, Cohen posits as follows in discussing DRM:

[t]he data processing paradigm conceals a power relationship, and that relationship, in turn, is a crucial determinant of the truth that data processing constructs. In evaluating knowledge claims about the processing of personally-identified data, we are not simply concerned with predictability and risk tolerance, but more fundamentally with questions of behavior modification and free will. Profiling represents not only a particular theory of

about what information or ideas one wishes to access as well as how they are used and communicated. If individuals believe that they are or may be monitored whenever they enjoy copyright works, or that their activities will be exposed to others by other means, even in the privacy of their homes, in many cases they will avoid accessing works, ideas and topic areas that they might otherwise wish to explore. Individuals' scope for autonomous action, including free thought, expression and creative endeavour inevitably shrinks as a result.²⁹⁵ Intellectual activity risks becoming stifled and homogenized.²⁹⁶ In terms of these impacts on creative

knowing, but also a disturbing, deeply cynical opportunism about the use of persuasion to reshape individual and collective knowledge. If data reveals truth, it is possible to attain omniscience. If data constructs truth, it is possible to attain power.

In each case (of the Panopticon and DRM), the act of surveillance, profiling and classification alters the present behaviour of the subjects and enables those in power to shape the future behaviour of the subjects. It is therefore essential that the subjects have little or no privacy in order for power to be exercised over them in these ways. Under the values described in this dissertation, such control would be considered unacceptable because we do not accept that individuals should have the power to control the minds of others. See e.g. *Stanley v Georgia*, *supra* note 281 at 559:

Whatever may be the justifications for other statutes regulating obscenity, we do not think they reach into the privacy of one's own home. If the First Amendment means anything, it means that a State has no business telling a man, sitting alone in his own house, what books he may read or what films he may watch. Our whole constitutional heritage rebels at the thought of giving government the power to control men's minds.

²⁹⁵ See e.g. Cohen, "DRM and Privacy", *supra* note 3 ("[Invasions of intellectual privacy] compromise rights of self-determination and undermine human dignity by eliminating the 'breathing space' for intellectual development" at 609).

²⁹⁶ For further reading on the homogenizing effects of surveillance, see generally David H Flaherty, *Protecting Privacy in Surveillance Societies* (Chapel Hill: The University of North Carolina Press, 1989); Jerry Kang, "Information Privacy in Cyberspace Transactions" (1998) 50 Stan L Rev 1193 at 1260; David Lyon,

endeavour, it should also be noted that it matters not whether observation of intellectual activities (whether by surveillance or other means) results in *accurate* inferences being drawn about individuals' thoughts. Individuals are averse to having their true thoughts known and to having thoughts improperly or unfairly attributed to them (i.e. being misjudged).²⁹⁷ The accuracy of the profiling is thus irrelevant because the effects of the interference on intellectual and creative endeavour are the same in either case.

The above harms to creative endeavour are unquestionably amplified in the information age, where there is a greater scope and amount of activity to be observed and where individuals are often unaware of the nature and extent of information about themselves being collected.²⁹⁸ The private sector and the state have new and

Surveillance Society: Monitoring Everyday Life (Buckingham: Open University Press, 2001). See also M Ryan Calo, "Unknown Unknowns: The Role of Innovation in Privacy" (29 October 2010) *Privacy and Innovation Symposium*, Yale Law School, Symposium Thought Pieces, online: Yale <http://www.law.yale.edu/documents/pdf/ISP/Yale_ISP_Calo.pdf> ("An absence of privacy can stifle individual or firm creativity. People are less creative in the moment when they perceive they are being observed and excessive monitoring may 'incline choices toward the bland and the mainstream'"), citing Cohen, "Examined Lives", *supra* note 13 and Richards, *supra* note 16.

²⁹⁷ Jeffrey Rosen, *The Unwanted Gaze: The Destruction of Privacy in America* (New York: Vintage Books, 2000) at 11-12 (privacy as protection against, among other things, misjudgment). On this point, it is also worth noting that reputational interests are directly related to privacy under the *Charter*, albeit in the defamation context where the information disclosed is false, which is different than a disclosure of true information about an individual's intellectual activities. See *Hill v Church of Scientology of Toronto*, *supra* note 146 ("...reputation is intimately related to the right to privacy which has been accorded constitutional protection" at 1133).

²⁹⁸ See e.g. *Canada (Privacy Commissioner) v Blood Tribe Department of Health*, 2008 SCC 44 ("Individuals are often unaware of the nature and extent of information about themselves being collected and stored by numerous private organizations, including employers. Some of this information may be quite inaccurate" at para 13), citing Ian B Lawson, *Privacy and Free Enterprise: The*

powerful ways of obtaining granular detail about individuals' intellectual activities. Marot would certainly be shocked to learn that third parties may not only find out what books individuals have in their library, but also what passages they read, how long they read them, whether they communicated them to others, etc., among myriad other discrete activities.²⁹⁹

Surveillance and interference can threaten the generation of new and potentially unpopular ideas, which can benefit from nurturing and testing before they are ready to be disclosed publicly. Intellectual privacy can be threatened in a number of ways, but one of the most important is through the disclosure or surveillance of records relating to reading, thinking, and non-public writing. In the past, such records have included letters, diaries, library records, and transcripts of phone conversations. But in the Information Age, the amount of such records has vastly increased, and includes new varieties, such as email, Internet browsing records, and search engine logs.³⁰⁰

Legal Protection of Personal Information in the Private Sector, 2d ed (Ottawa: Public Interest Advocacy Centre, 1997) at 32:

Not only is information circulated from unknown or out-of-date sources, but it is mixed and matched with other information purportedly relating to the same individuals. Digitalized attributes of one consumer may be mixed and matched with those of others who subjectively appear to belong to the same category of socioeconomic behaviour. Few data "subjects" ever see the information being held and exchanged under their names; fewer still are able to correct this information or have it withdrawn from circulation.

²⁹⁹ See generally Chapter 1. See also Lessig, *Code version 2.0*, *supra* note 24 ("[Digital technologies] not only make more behavior monitorable; they also make more behavior searchable. [...] Thus, increasingly life becomes a village composed of parallel processors, accessible at any time to reconstruct events or track behavior" at 203).

³⁰⁰ Richards, "Brandeis", *supra* note 240 at 1347.

The harms to values of autonomy, identity, expression and creative endeavour that flow from absence of intellectual privacy as described above thus reinforce the connection between those values and intellectual privacy, help distinguish intellectual privacy from other forms of privacy, and demonstrate reasons why it is important that intellectual privacy be protected.³⁰¹

IV. Some Limits of Intellectual Privacy

'Here we are ladies. The mother of all libraries!' [...] '[T]he institute does require that you submit periodic reports to track what you're doing. In exchange for that harmless invasion of intellectual privacy, one is granted free and full access to all that is housed here.'³⁰²

³⁰¹ Waldo, Lin, & Millett, *supra* note 22 at 236:

[A] privacy interest in one's intellectual pursuits is arguably different from an interest in maintaining the confidentiality of one's medical records or in resisting broad law enforcement surveillance tactics for privacy reasons. While one might worry about embarrassment resulting from the disclosure of medical information, or about interference by government or law enforcement in the study of politically or socially unacceptable ideas, the concern for intellectual privacy also rests on a more general fear of the ostracism, ridicule, or loss of social status that could result if the subject matter of inquiry were generally known. The kind of privacy that libraries seek to guarantee also is different from the kind of privacy that might be needed by the patron of an abortion clinic, pawnshop, or drug rehabilitation center. In those other cases, the privacy interest extends to the actual use of the service being provided. In the case of the library, worries about privacy do not center on the fact that a person is a patron of a library, but rather about the content of that patron's use.

³⁰² C G McGovern-Bowen, *Evil Seed* (Westlake Village: Westlake Publishers, 2001) at 312-13.

Part III of this chapter explored what intellectual privacy is and what values are interrelated with the concept, including some of the ways that it is distinct from other conceptions of privacy. However, the discussion about intellectual privacy in this chapter should not be read as suggesting that intellectual privacy is absolute. Like other forms of privacy, there are a variety of important circumstances where it appears there are good reasons to balance intellectual privacy with other interests. Such circumstances may include litigation,³⁰³ law enforcement,³⁰⁴ and media inquiries, which may also implicate values of freedom of expression. Indeed, broad limitations may also be appropriate where they protect other constitutional values (e.g. restrictions are placed on private possession of child pornography, at least in part, because the material itself implicates the privacy and equality rights of those whose abuse is depicted in it).³⁰⁵

Public figures and those in power,³⁰⁶ for example, may not be entitled to invoke intellectual privacy in cases where citizens have a *bona fide* public interest in holding such individuals to account. Indeed, intellectual privacy has been characterized as a negative value in some cases where transparency and accountability are required. In 1984, after Lord Chief Justice Lane refused to permit

³⁰³ See generally Cameron & Teehan, *supra* note 162.

³⁰⁴ See generally Kerr & Cameron, "Nymity, P2P & ISPs", *supra* note 59.

³⁰⁵ I am grateful to Jane Bailey for alerting me to this broader point.

³⁰⁶ See e.g. Robert Burton, *The Anatomy of Melancholy*, 1621, Holbrook Jackson, ed, (New York: New York Review of Books, 2001) at 149:

Look how many servants he hath, and so many enemies he suspects; for liberty he entertains ambition; his pleasures are no pleasures; and that which is worst, he cannot be private or enjoy himself as other men do, his state is a servitude. A countryman may travel from kingdom to kingdom, province to province, city to city, and glut his eyes with delightful objects, hawk, hunt, and use those ordinary disports, without any notice taken, all which a prince or a great man cannot do.

further research into the sentencing practices of judges (which involved questions about family background and other matters), Hugo Young stated the following in the Guardian:

Lord Lane has enshrined ignorance as a judicial virtue and intellectual privacy as the hallmark of the priesthood over which he presides. Rarely have such eminent heads been so piously buried in the sand, and never, I would hazard, at such social cost.³⁰⁷

More recently, the Chief Justice of the Wisconsin Supreme Court suggested that judges' deliberations about which cases to take and how to decide them should be performed in the open so that such processes are transparent to the public.³⁰⁸

Intellectual privacy has also been criticized as a negative value where it is used by the knowledgeable to hold and profit from their own private knowledge: "Boyle condemned 'the avarice' of those 'secretists' who secured profit through the practice of intellectual privacy. Both Christian charity and civic virtue demanded that useful knowledge circulate in the public domain, for the public benefit."³⁰⁹

In addition, as suggested by the quote at the outset of this part, there may be some circumstances where intellectual privacy might attempt to accommodate some of the very values that are

³⁰⁷ Hugo Young, *The Guardian* (14 September 1984), cited in Andrew Ashworth, "Sentencing and Sensitivity: A Challenge for Criminological Research" in Lucia Zedner & Andrew Ashworth, eds, *The criminological foundations of penal policy: essays in honour of Roger Hood* (Oxford: Oxford University Press, 2003) 295 at 323, n 95.

³⁰⁸ See generally Adam Cohen, "Justice on Display: Should Judges Deliberate in Public?" *Time* (12 September 2011), online: Yahoo <http://old.news.yahoo.com/s/time/20110913/us_time/08599209273800>.

³⁰⁹ Steven Shapin, *A Social History of Truth: Civility and Science in Seventeenth-century England* (Chicago: University Of Chicago Press, 1994) at 175.

interrelated with it. For example, sharing records of intellectual activity may in some cases advance the objectives of copyright and development of new ideas by aiding subsequent researchers.³¹⁰ Such records may include comments and ratings of works, identification of commonly cited passages in works, identification of the areas of a work where many researchers/readers have spent the most time, other books purchased by readers of the works, etc. There is a body of existing research discussing how these “interaction histories” can permit subsequent users to “derive meaning from the record.”³¹¹ However, it is also recognized that individuals’ intellectual privacy interests must be carefully addressed:

...there is also a possible concern about the rights of the user to intellectual privacy. In the case of academics working with text collections related to their field of expertise, it may be possible that activities such as sorting, grouping, and subsetting the material are a form of professional engagement that should not by default be made available to subsequent users, since these actions may provide insights into the collection that could prove of value, and their introduction into an interaction history may constitute a form of public release that is inappropriate. In this case, the ability of the user to decide whether or not to store the interaction history may prove to be a necessary feature for these kinds of collections.

On the other hand, it may also happen that people who are recognized authorities in a given field are willing to

³¹⁰ Indeed, the failure to share such information can in some contexts result in allegations of plagiarism or academic dishonesty.

³¹¹ See generally Stan Ruecker, “Traces of Previous Use: The Communicational Possibilities of Interaction Histories” in Jorge Frascara, ed, *Designing Effective Communications: Creative Contexts for Clarity and Meaning* (New York: Allworth Press, 2006) at 270, 277.

create, edit, annotate and store interaction histories that are in some way associated with them as scholars. Such activity would then become part of the public record of the work of these people, and could be duly noted within the collection. A parallel example in the analog world exists in the form of library catalogs of personal libraries of famous writers or academics.

An alternative strategy is to provide the user with a method that allows for personal storage and re-access of the interaction history, without making the record public. For this to be possible, it would also be necessary to store enough information about the user to secure subsequent access, either through a password system or a browser cookie or some similar method.³¹²

Limits on intellectual privacy such as those expressed above will be further explored in Chapter 5 as it is important that any such limits be reflected in the solutions proffered herein. It is also imperative that two further limits of the concept of “intellectual privacy” be mentioned at this time.

First, there is the challenge of scope, or what Marc Blitz calls the “where” of intellectual privacy.³¹³ There are a variety of activities which may be indicative of an individual’s thinking but which do not involve creative works.³¹⁴ For example, the fact that an

³¹² *Ibid* at 277.

³¹³ Blitz, *supra* note 110 at 17:

What kinds of activities count as “close prox[ies] for thought” of the kind that should be covered by intellectual privacy protections? This is a difficult question, one that is a little more troublesome than [Neil Richards] acknowledges. It is not merely about more precisely mapping the blurry outer boundaries of the realm of activity that qualifies for privacy protection. It is about understanding what kind of logic, principle, or convention justifies such borders in the first place.

³¹⁴ See e.g. Slobogin, *supra* note 110 at 25:

individual purchases organic produce may be a powerful indicator of their thoughts in respect of nutrition and personal health. Purchasing habits can suggest inferences to be drawn about individuals' thoughts in different contexts, perhaps even more directly than reading material might. Protecting individual's privacy interests in such activities may therefore be thought to promote some of the same values that are interrelated with intellectual privacy; at the same time, however, it must be acknowledged that (a) such activities are not "intellectual" in the sense identified in Part III of this chapter, (b) they do not share the same connection with freedom of thought, expression and creative endeavour that is shared between intellectual privacy and those values in the context of copyright works, and (c) in many cases, they are arguably adequately governed by privacy laws of general application.³¹⁵

Although Richards says that intellectual privacy impinges on only a "fraction" of the issues connected with privacy, in fact, virtually all of our activities can be said to enhance freedom of thought and intellectual exploration. Richards focuses on what he calls "intellectual records" such as lists of Web sites visited, books owned, and terms entered into search engines, differentiating these activities from purchases of consumer goods. But if the latter purchases consist of religious foods, war video games, or certain brand names, or if information about all of an individual's purchases are aggregated, that person's belief system might be revealed just as clearly as if all of her Internet travels were accessed.

³¹⁵ See e.g. *ibid* at 25-26:

[M]any types of sources that Richards considers *prima facie* "intellectual" in nature may not be. Many Web site lists consist entirely of URLs for commercial companies, the books on one's shelves may all be mysteries, and the national security letters that Richards believes are anathema to intellectual privacy are usually aimed solely at obtaining financial information. Perhaps we could come up with categories of intellectual privacy, organize them into a hierarchy of privacy, and apply the

Second, there is the issue of consent. In other words, there are a variety of circumstances, particularly in the information age, where individuals willingly and openly expose their intellectual activities to others. When intellectual privacy is cast in this way as a legal right, as opposed to a state of being, it must be acknowledged that there is no violation of the right where it has been knowingly surrendered by the individual. Individuals should (in many or all cases) have the power to choose whether to legally consent to a diminishment of their state of intellectual privacy. The solutions described in Chapter 5 account for this issue by proposing measures that are aimed at ensuring that individuals are sufficiently informed about the choices they are being asked to make when it comes to their intellectual privacy, that they provide meaningful consent, and that there are strong incentives for copyright holders and others to ensure that individuals give informed consent. Given the widespread use of standard form terms of service and other “agreements” which include consent provisions (but which individuals almost never read or understand) cracking the consent issue is one of the most important aspects of any legal system of privacy protection, including in relation to intellectual privacy.³¹⁶ While the matter of consent is not

hierarchy ex ante, but ex post we are likely to find that we have been both under- and over-inclusive.

³¹⁶ See e.g. David A Anderson, “Privacy and Fictitious Contracts” (2009) 87 Tex L Rev 11 at 14:

Professor Richards suggests several steps to ameliorate this situation, including requiring notification of individuals when their data is sold, limiting uses to which data can be put and periods for which it can be retained, and forbidding disclosure of “particularly sensitive types of intellectual data.” In my estimation, that response is far too tepid. The problem is that the law allows private entities to coerce us into furnishing information under the fiction that we are providing it voluntarily. That is the problem that must be attacked. If we accept the legitimacy of that construct, trying to control the uses to which our information is put will always be a struggle. The

unique to intellectual privacy, the solutions described in Chapter 5 are custom-designed for intellectual privacy in the copyright context.

information becomes a business asset, and the ingenuity, perfidy, and persistence of those who wish to exploit the asset will usually defeat attempts at regulation. We all learn eventually that the only sure way to keep secrets is to not share them. We also know that modern life makes that very hard to do. But the fiction that we voluntarily agree to disclose almost anything that the purveyors of the accoutrements of modern life demand to know makes the control of secrets harder than it needs to be.

CHAPTER 3:

CONTEMPORARY CONFLICT BETWEEN

COPYRIGHT AND INTELLECTUAL

PRIVACY

The ultimate aim of this dissertation is to explain why and how intellectual privacy ought to be addressed in copyright. In furtherance of achieve this objective, it is important to have a general understanding of the ways that copyright and intellectual privacy have come into conflict in recent years. The examples of conflict described in this chapter are, on their face, problems spawned by the use of digital technologies in association with copyright works, such as the examples of eReader and Google Books discussed in Chapter 1. Technology examples are certainly important markers of conflict between copyright and intellectual privacy but they are not the only area of conflict. Conflict between copyright and intellectual privacy is Gordian in much the same way that both copyright and privacy are independently complex concepts.

This chapter describes conflict between copyright and intellectual privacy in three conceptual categories: technology, law and

intermediaries.³¹⁷ The conflict can be more easily understood through these three themes and through an appreciation of the overlap and connections between them.³¹⁸ We begin with technology and then consider law and intermediaries.

I. Technology

A wide variety of technologies have long been used by copyright holders and others to intermediate individuals' access to and enjoyment of copyright works. Other than during a live performance of a work, access to works is dependent on a variety of technology media and playback devices. Books, magazines, newspapers, player pianos, projectors, LPs, radios, televisions, cassette tapes, mini discs, CDs, VCRs, video cassette tapes, DVDs, BluRay Discs, iPods, computers, portable drives, e-book readers and many other technologies form the ways that we access and enjoy copyright works. Increasingly, our personal computers play a central role in our access to copyright works in digital form on the Internet. The myriad technologies between individuals and copyright works have a variety of implications for privacy. The following sections briefly review several of these contemporary technologies and their implications for privacy.

³¹⁷ The laws discussed in this chapter are copyright-related laws. For example, this chapter does not discuss how data protection laws can bear on the conflict between copyright and intellectual privacy. Chapter 5 discusses the application of data protection law and other areas of law, including a review of how other areas of law might inform how copyright ought to internally account for intellectual privacy.

³¹⁸ For example, as described in this chapter, components of DRM are sometimes protected by anti-circumvention laws. Contracts are also an integral component of DRM, thus linking contract law to technology.

A. TPMs and RMI

The term “technological measure” was introduced in 1996 in connection with its inclusion in two international intellectual property treaties - the *WIPO Copyright Treaty*³¹⁹ and the *WIPO Performances and Phonograms Treaty*³²⁰, known collectively as the “WIPO Treaties.”³²¹ Technological measures are commonly called “technological protection measures” or TPMs. TPMs are technologies that function to control access to or use of copyright works, or both.³²² TPMs are one of the building blocks of DRM systems.

TPMs can range in sophistication from simple username and password-protections to complex encryption measures. For example, an encryption TPM might encrypt a copyright work and then permit it to be accessed by only those individuals or devices that have been approved by the copyright holder.

TPMs that control access to copyright works are sometimes called ‘access controls’. These technologies act as gatekeepers to a copyright work; they do not control what can be done with a work after access is achieved. An access control might be thought of as the ticket window at a movie theater: the ticket window ensures that individuals get access to the movie only after they have

³¹⁹ 20 December 1996, 2186 UNTS 121, WIPO Publication No 226 (entered into force 6 March 2002) [WCT].

³²⁰ 20 December 1996, 2186 UNTS 203, WIPO Publication No 227 (entered into force 20 May 2002) [WPPT].

³²¹ See Canadian Heritage, News Release, “Canada Commits to Sign International Copyright Treaties” (18 December 1997), online: Heritage Canada
<http://www.pch.gc.ca/newsroom/index_e.cfm?fuseaction=displayDocument&DocIDCd=7NR135>. The pertinent provisions of these treaties are discussed in Part II(B) of this chapter.

³²² See generally Kerr, Maurushat & Tacit, “TPMs Part I”, *supra* note 32.

purchased a ticket. However, the ticket window does not control what individuals do once they are inside the venue enjoying the copyright work. Inside, individuals are free to purchase popcorn, choose and change their seat, and use the restroom, among other activities.³²³

The Content Scrambling System (CSS) is an example of an access control TPM. CSS scrambles content on DVDs and permits playback of the CSS-protected DVDs (i.e. grants access) only on DVD players made by manufacturers that license the right to include CSS descrambling software in their players.³²⁴ The Advanced Access Content System (AACS) is a next-generation access control that provides similar but improved access control for Blu-ray Discs.³²⁵

TPMs that control how copyright works can be used are sometimes called 'rights controls'.³²⁶ These technologies do not regulate access to works. Instead, they control the ways that an individual can use a copyright work once the individual has access to it. The most common form of rights control TPM is a copy-control TPM. Copy control TPMs limit or prohibit copying of copyright works. For example, if an individual copies a DVD movie protected by Macrovision copy-control technology, the resulting copy of the movie will be degraded or non-functional as a result of the

³²³ The movie theatre experience described in this sentence reflects the practice in North America. I am grateful to Ian Kerr for reminding me of this point and for noting that in at least some theaters in Spain, for example, individuals are assigned specific seats on their ticket.

³²⁴ DVD Copy Control Association, "Frequently Asked Questions," online: DVD CCA, <<http://www.dvcca.org/faq.html>>. See also *Universal City Studios, Inc v Corley*, 273 F3d 429 (2d Cir NY 2001) at 436-437.

³²⁵ AACS Licensing Administrator, "How AACS Works," online: AACS <http://www.aacsla.com/what/how_aacs_works/>.

³²⁶ See generally Anthony R Reese, "Legal Incentives for Adopting Digital Rights Management Systems: Merging Access Controls and Rights Controls" (2003) 18 Berkeley Tech LJ 619.

operation of the Macrovision TPM.³²⁷ In this example, the individual is able to access and play the movie on the original DVD. Macrovision does not control access to the movie. However, Macrovision does restrict the ability of the individual to copy the movie by analog means, for example through the use of a video cable connected between a playback device and a recording device.

Similar copy-controls exist in the cable industry where a Copy Control Information (CCI) byte is linked to copyright television broadcasts in order to control copying using digital video recorders such as TiVo.³²⁸ Such devices are designed to recognize and adhere to the rules spelled out in the CCI that accompanies the broadcast. CCI has four forms: copy free (00), copy once (01), copy no more (10) and copy never (11). 'Copy free' information tells the individual's device that the content can be copied without restriction. 'Copy once' permits the individual to make one copy. If 'copy once' content is copied, then the CCI of the content becomes 'copy no more'. 'Copy never' indicates that copying of the content is prohibited. CCI is different than the 'broadcast flag' proposal in the United States. Had it been adopted, the 'broadcast flag' was a simple on/off flag that would have indicated to devices whether content could be redistributed without restrictions.³²⁹

The difference between controlling access to and use of copyright works is an important distinction that bears on the implications that TPMs can have for copyright, for privacy and for the way that conflict between the two is resolved. The distinction and the

³²⁷ Macrovision, "Protecting Your Content from Analog Copying and Piracy," online: Macrovision <http://www.macrovision.com/products/activereach_dvd/acp/index.shtml>.

³²⁸ See TiVo, "Questions about copy protection," online: TiVo <http://www.tivo.com/setupandsupport/technicalsupport/helpwithtivofeatures/Questions_About_Copy_Protection.html>.

³²⁹ For discussion of the broadcast flag, see *Am Library Ass'n v FCC*, 365 US App DC 353 (2005) at 357.

integral interplay between access and use is a thread that runs throughout this dissertation.

In addition to TPMs, rights management information (RMI) is one of the building blocks of DRM and introduced to the copyright lexicon as a result of the WIPO Treaties.³³⁰ In general terms, RMI refers to a particular class of information attached to a copyright work or that otherwise appears in connection with the communication of a work to the public. As its name suggests, RMI is information that facilitates the management of copyright in a work, including the identity of the author, the identity of the copyright holder, information that identifies a work, and information about how a work may or may not be used.³³¹

When one combines an access control TPM, a rights control TPM and RMI, one has the makings of a DRM system. Different forms of TPMs are often used together and in combination with other components, including RMI, to create advanced management systems for copyright works: DRM systems.³³² Understanding TPM

³³⁰ See WCT, *supra* note 319, art 12. RMI is sometimes called “copyright management information” or CMI. See e.g. *Digital Millennium Copyright Act of 1998*, 17 USC § 1201, § 1202 [DMCA].

³³¹ See e.g. WCT, *ibid*:

‘rights management information’ means information which identifies the work, the author of the work, the owner of any right in the work, or information about the terms and conditions of use of the work, and any numbers or codes that represent such information, when any of these items of information is attached to a copy of a work or appears in connection with the communication of a work to the public.

³³² See Guibault et al, *supra* note 29 at 14:

The fundamental difference between DRM and TPMs is that TPMs generally are designed to impede access or copying. DRM systems do not impede access or copying per se, but rather create an environment in which various types of use, including copying, are only practically possible in compliance with the contractual terms set by the rights holders. DRM is used to

and RMI as building blocks of DRM is important because it is these building blocks that are typically protected by anti-circumvention laws as discussed below. The next section provides a brief overview of DRM systems.

B. DRM

DRM technology is the subject of an extensive and growing body of multi-disciplinary literature.³³³ For the purposes of describing the privacy threats posed by DRM in the copyright context, it is not necessary to conduct a detailed analysis or review of DRM literature. Nor is it necessary to possess a detailed understanding of how DRM functions at a technical level. This section is intended to

manage access to content by combining TPMs with elements such as payment mechanisms, customer management and authorisation schemes.

See also Mark Stamp, "Digital Rights Management: The Technology Behind the Hype" (19 December 2002) [unpublished], online: <<http://home.earthlink.net/~mstamp1/papers/DRMpaper.pdf>>.

³³³ See e.g. European Committee for Standardization and Information Society Standardization System, "Digital Rights Management: Final Report" (September 30, 2003) at 27-69, online: Europa <<http://europa.eu.int/comm/enterprise/ict/policy/doc/drm.pdf>>; Paul Petrick, "Why DRM Should be Cause for Concern: An Economic and Legal Analysis of the Effect of Digital Technology on the Music Industry" (November 2004) Berkman Center for Internet & Society, Research Publication No. 2004-09; Renato Iannella, Rights Management and Licensing Multimedia Services" in George A Tsihrintzis and Lakhmi C Jain, eds, *Multimedia Services in Intelligent Environments*, (Berlin: Springer-Verlag, 2008) at 327-349; Carlisle E George, "Copyright Management Systems: Accessing the power balance" in Chris Zielinski, Penny Duquenoy, & Kai Kimppa, eds, *The Information Society: Emerging Landscapes* (Boston: Springer, 2006); Jean Camp, "DRM: Doesn't Really Mean Digital Copyright Management" (August 2002) KSG Working Paper Series RWP02-034; Timothy Armstrong, "Digital Rights Management and the Process of Fair Use" (2006) 20 *Harvard Journal of Law & Technology* 49; Kerr, Maurushat & Tacit, "TPMs Part I", *supra* note 32; Kerr, Maurushat & Tacit, "TPMs Part II", *supra* note 32.

provide a basic introduction to DRM and, in the next section of this chapter, to build on the material included in the Introduction to this dissertation by describing some of the important privacy issues that DRM and its component technologies can raise.

'DRM' is a term commonly used to refer to technological systems used by copyright holders and others to automatically regulate access to and manage rights in relation to information, including copyright works. DRM is a form of persistent technological protection that is tied to copyright works at all times, no matter where the works are located or who has possession of them.³³⁴ DRM typically functions to control copyright works, principally to collect payments for uses of works and to prevent works from being accessed or used in unauthorized ways.³³⁵

DRM can be thought of as being like an electronic railway conductor for copyright works. The conductor ensures that you don't get on board the train without a ticket (i.e. access control) and then, while on board, the conductor accompanies and attends to you throughout your (intellectual) journey (i.e. monitors your activities) to ensure (i.e. rights control) that you enjoy the ride in accordance with all the rules (i.e. license terms) of the railway. If you want a meal on board or if you want to enjoy the ride in a sleeping car, then the conductor might charge you a little extra for those features. A 'DRM conductor' might go a little further though.

³³⁴ See Mark Stamp, "Risks of digital rights management" (2002) 45 Communications of the ACM 120 (discussing DRM as a form of "remote control" over works after the works have been delivered to users). See also Nic Garnett, "Automated Rights Management Systems and Copyright Limitations and Exceptions" (Paper delivered at WIPO, Standing Committee on Copyright and Related Rights, Fourteenth Session, Geneva, May 1 – 5, 2006, SCCR/14/5, 27 April 2006).

³³⁵ See generally Niels Rump, "Digital Rights Management: Technological Aspects-Definition, Aspects, and Overview" in Eberhard Becker et al, eds, *Digital Rights Management-Technological, Economic, Legal and Political Aspects* (Berlin: Springer-Verlag, 2003). See also Guibault et al, *supra* note 29.

On a DRM train, the conductor might control your ability to look out the window, talk to your fellow passengers, sleep, write, read, do a crossword puzzle, use the restroom, bring your own food or water on board, take photographs, or engage in any number of other conceivable activities that individuals are typically free to do on board real-world trains. Of course, the DRM conductor might permit you to engage in some of these activities provided that you pay for permission to do so.

The conductor metaphor is imperfect and intended to provide only a general illustration of how DRM can operate. The point of the metaphor is that DRM can be used to enforce any number of conceivable restrictions on access to and use of copyright works and that some restrictions might seem perfectly acceptable to us while others may not.³³⁶ Through DRM, copyright holders and others can control activities that they have never been able to control before, including some that copyright law may not give them the right to control.³³⁷

³³⁶ As discussed in Chapter 5, this statement highlights the importance of approaching intellectual privacy in a normative manner. A failure to do so will mean that what is unacceptable today may become the norm of tomorrow.

³³⁷ For example, DRM enables control over activities that would otherwise be fair dealing under copyright law and control over works in which copyright protection has expired. See generally, Dan Burk & Julie Cohen, "Fair Use Infrastructure for Rights Management Systems" (2001) 15 Harv J & Tech 41; Deirdre Mulligan & Aaron Burstein, "Implementing Copyright Limitations in Rights Expression Languages" in Joan Feigenbaum, ed, *Digital Rights Management: ACM CCS-9 Workshop, DRM 2002, Washington, DC, USA, November 18, 2002, Revised Papers* (New York: Springer, 2002) 137; Yee Fen Lim, "Digital Rights Management: Merging Contract, Copyright and Criminal Law" in Reihaneh Safavi-Naini & Moti Yung, eds, *Digital Rights Management. Technologies, Issues, Challenges and Systems* (Berlin: Springer, 2006) 66 (arguing that DRM gives copyright holders something akin to tangible property rights more powerful than copyright law permits).

DRM can enforce a wide variety of permissions in association with copyright works such as 'read, but don't copy', 'read, but don't print', 'read, but only copy five times', 'read, but don't copy any text', 'read on one device only and do not copy to other devices', or 'play only on devices purchased in Canada'. For example, Sony has utilized a technological measure that ensures its PlayStation games can only be accessed on its game consoles that are purchased in the same geographic region.³³⁸ As these examples suggest, DRM-protected content typically comes packaged with a standard form license agreement that spells out how a work can and cannot be used. DRM then automates the management and enforcement of the terms of the license, metering out access to and use of works strictly in accordance with the terms of the license.³³⁹ DRM is essentially a contract combined with technology.³⁴⁰

DRM can be comprised of several technological components that include TPMs, RMI, a rights expression language, digital watermarking, digital fingerprinting, digital signatures and payment systems.³⁴¹ At a base level, however, DRM systems

³³⁸ See generally *Stevens v Kabushiki Kaisha Sony Computer Entertainment & Ors*, [2005] HCA 58.

³³⁹ See generally Kerr & Bailey, *supra* note 60; Julie Cohen, "Copyright and the Jurisprudence of Self-Help" (1998) 13 Berkeley Tech LJ 1089.

³⁴⁰ Hugenholtz characterizes DRM as a contract combined with technology. See Bernt Hugenholtz, "Copyright, Contract and Code: What Will Remain of the Public Domain" (2000) 26 Brook J Int'l L 77. See also Daniel Gervais, "Electronic Rights Management and Digital Identifier Systems" (1999) 4 The Journal of Electronic Publishing 3 [Gervais, "Electronic Rights Management"] Guibault et al, *supra* note 29.

³⁴¹ See generally Rump, *supra* note 335 at 3, 9; Guibault et al, *supra* note 29; Mulligan & Burstein, *supra* note 337 at 137; Bill Rosenblatt, "Sony Music Gets Fingerprinted" *DRM Watch* (3 June 2004), online: *DRM Watch* <<http://www.drmwatch.com/drmtech/article.php/3363151>>; US, *Information Infrastructure Task Force, Intellectual Property and the National Information Infrastructure: The Report of the Working Group on Intellectual Property Rights*, (September 1995) at 187, online: US Patent and Trademark Office <<http://www.uspto.gov/web/offices/com/doc/ipnii/ipnii.pdf>> [NII, White

contain two central components: first, they contain databases of identifying and other information about copyright works, their owners and individuals that access and use works, and second, they contain licensing or other tools to regulate access and to manage licensed permissions.³⁴²

In order to manage rights, DRM usually requires individuals to disclose personal information to content providers when registering for a product or service. This information might include their name, email address, age, sex, mailing address, and credit card information.³⁴³ Microsoft's description of DRM describes this collection of information from individuals as one of the features of DRM:

[...] Digital rights management enables content providers to protect their content and maintain control over distribution. Content providers can protect and manage their rights by creating licenses for each digital media file. License registration procedures also give these companies important customer information. Such information helps content providers stay closer to their customers. [...]³⁴⁴

Information about individuals' access to and enjoyment of creative works is unquestionably valuable to copyright holders and others since it can be used to generate additional revenue streams, for example, through advertising and marketing.³⁴⁵ A number of

Paper]; Dean S Marks & Bruce H Turnbull, "Technical Protection Measures: The Intersection of Technology, Law and Commercial Licences" (2000) 22 Eur IP Rev 198 at 212.

³⁴² See generally Gervais, "Electronic Rights Management", *supra* note 340.

³⁴³ See the discussion in the next section of this chapter.

³⁴⁴ Microsoft, "Windows Media DRM FAQ" (October 2005), online: Microsoft <<http://www.microsoft.com/windows/windowsmedia/forpros/drm/faq.aspx>>.

³⁴⁵ See generally Chris J Hoofnagle, "Digital Rights Management: Many Technical Controls on Digital Content Distribution Can Create a Surveillance

intermediaries utilize information about individuals' access to and use of copyright works in order to recommend other products to the same individuals and to others. iTunes and Amazon both provide recommendations based on individuals' listening, reading and purchasing history. This information is also used to suggest recommendations to other individuals who search for or purchase particular products. We are increasingly familiar with the phrases "Customers Who Bought This Item Also Bought" and "What Do Customers Ultimately Buy After Viewing This Item?" used by Amazon.com to market products to individuals that view items on the Amazon site. Canada's largest book retailer, Indigo Books and Music, is explicit about its intention to track individuals' e-book reading habits in order to market additional products to the individuals: "...we basically need to see how and what you read. [...] We'll know exactly what you're reading, how often, whether you've read the whole book that you've bought or not, taking that engagement information into account to provide great recommendations..."³⁴⁶ Finally, Google's online advertising service also utilizes information about individuals' online activities, including their browsing and viewing habits³⁴⁷ and their use of Google Books, in order to deliver advertisements.³⁴⁸

Society" (2004) 5 Colum Sci & Tech L Rev 1 at 3; Mulligan, Han & Burstein, *supra* note 32 at 82-83; Cohen, "A Right to Read Anonymously", *supra* note 45. See also Guibault et al, *supra* note 29. See also Chapter 1 and Part I(C) of this chapter. Stephanie Clifford, "Your Online Clicks Have Value, for Someone Who Has Something to Sell" *New York Times* (March 25, 2009), online: New York Times <<http://www.nytimes.com/2009/03/26/business/media/26adco.html>>.

³⁴⁶ James Adams, "Indigo launches e-book service" *Globe and Mail* (25 February 2009) at R1 (quoting Michael Serbinis, Indigo Vice President IT).

³⁴⁷ Maija Palmer, "Google to match ads with viewing habits", *Financial Times* (11 March 2009), online: *Financial Times* <<http://www.ft.com/cms/s/0/2fc07804-0e4b-11de-b099-0000779fd2ac.html>>. See also the discussion in Part III of this chapter.

³⁴⁸ This issue is discussed in Chapter 1.

In light of how valuable information about individuals' intellectual activities can be,³⁴⁹ it is not surprising that technologies that help us search for, access and enjoy copyright works can raise a number of important privacy issues. These are discussed in the next section.

C. Impact of DRM on Intellectual Privacy

In fulfilling its protective and rights management roles, DRM typically contains monitoring and reporting functionality.³⁵⁰ These functions permit copyright holders to track accesses and uses of their works and, through the DRM, to automatically grant or refuse permissions and to collect payments.³⁵¹ Identification and authentication of individuals or devices endeavoring to access or use works is a key part of many DRM systems. In other words, DRM needs to know whether the person requesting access or use of a work is a person who has authorization to do so.³⁵² To achieve this objective, many DRM systems monitor individuals' attempts to

³⁴⁹ In 2008, Google's advertising revenues topped 21 billion dollars. Google, "2008 Income Statement", online: Google <http://investor.google.com/fin_data.html>.

³⁵⁰ See NII, *White Paper*, *supra* note 341 ("These systems will serve the functions of tracking and monitoring uses of copyrighted works as well as licensing of rights and indicating attribution, creation and ownership interests" at 191); Rump, *supra* note 335 at 4; Kerr & Bailey, *supra* note 60 at 89-91; Kerr, Maurushat & Tacit, "TPMs Part I", *supra* note 32 at § 5.2.2; Bygrave, "Digital Rights Management and Privacy", *supra* note 32 at 418-446; Mulligan, Han & Burstein, *supra* note 32 at 77.

³⁵¹ See Rump, *supra* note 335; Jeffrey P Cunard, "Technological Protection of Copyrighted Works and Copyrighted Management Systems: A Brief Survey of the Landscape" (Paper delivered at the ALAI Congress, 2001) at 2, online: ALAI <www.alai-usa.org/2001_conference/pres_cunard.doc>; Lessig, *Code version 2.0*, *supra* note 24 at 191.

³⁵² See generally Gervais, "Electronic Rights Management", *supra* note 340. See also Lessig, *Code version 2.0*, *ibid* (noting that trusted systems are dependent on information about how products are used and thus need to track and monitor).

access or use a work. Before granting permission for such access or use, DRM verifies individuals' identities against a database of permissions associated with the individual and the work.³⁵³

DRM offers an unprecedented potential to create detailed profiles of individuals' private reading, viewing, listening, searching and browsing habits, often without the individual being aware that they were the subject of monitoring. Napster, for example, explains that its DRM software monitors how many copies of a work an individual makes as well as how many times the individual plays a downloaded song, even though the user in fact pays a subscription fee for unlimited downloads and listening, not a pay-per-play fee:

A "Download" is a Track that you may save to the hard drive of your personal computer and play back as many times as you want for so long as your subscription is current. You may make an unlimited number of Downloads while your subscription is current. You may copy each Download to up to two additional personal computers that you own (i.e. a total of 3 copies). [...] The Client will count the number of times that you play a Download, including while you are offline, for royalty accounting and analysis purposes.³⁵⁴

Similar monitoring of individuals' access to and enjoyment of works is found in the service offered by Bookshare.org. Bookshare.org is a non-profit entity that provides access to books and periodicals for individuals with visual or other print disabilities. Bookshare.org provides a "library" of material and "believes that people with print disabilities should have the same ease of access to books and periodicals that people without

³⁵³ Hoofnagle, *supra* note 345 at 2, 3.

³⁵⁴ Napster, "Terms and Conditions" (30 June 2006), online: Napster <<http://www.napster.com/terms.html>>.

disabilities enjoy.”³⁵⁵ However, unlike a traditional library, Bookshare.org's privacy policy makes clear that it embeds identifying information in the materials that it distributes and tracks use of the materials for a number of purposes:

Bookshare.org will also maintain transaction logs of the materials downloaded by its users. We will use this information for the following purposes:

To flag usage that is potentially in violation of our terms of use or the copyright law.

In cases of suspected abuse where copyrighted Content has been made available to unqualified individuals, to trace copyrighted Content back to the user using user-identifiable information embedded in downloaded Content.

To provide users with information about the Content downloaded under their accounts.

To gather statistical data about usage patterns for the improvement of the Bookshare.org service.

Possibly, to provide suggested content based on the users past reading patterns.

We will not provide access to any third parties to the information contained in our transaction logs, except in connection with investigation of or for actual legal proceedings concerning potential abuse. [...] ³⁵⁶

³⁵⁵ Bookshare.org, “Welcome”, online: Bookshare <<http://www.bookshare.org/web/Welcome.html>>.

³⁵⁶ Bookshare.org, “Privacy Policy” (29 January 2004), online: Bookshare <<http://www.bookshare.org/web/Privacy.html>> [emphasis added]. Bookshare.org's security program is described in Garnett, *supra* note 334 at 51-54.

The potential privacy implications of DRM are now relatively widely recognized and increasingly well-documented.³⁵⁷ For example, privacy is one of five major categories of concerns identified in the European Community as being a barrier to consumer acceptability of DRM.³⁵⁸ The EU Data Protection Working Party has also expressed concern about the privacy implications of DRM in so far as it can be used to track and profile individuals' activities:

The Working Party is concerned about the fact that the legitimate use of technologies to protect [copyright] works could be detrimental to the protection of personal data of individuals. As for the application of data protection principles to the digital management of rights, it has observed an increasing gap between the protection of individuals in the off-line and on-line worlds, especially considering the generalised tracing and profiling of individuals.³⁵⁹

³⁵⁷ See generally Barry Sookman, "'TPMs': A Perfect Storm for Consumers: Replies to Professor Geist" (2005) 4 Can J L & Tech 23 ("There is no doubt that business models that involve metering uses of content could involve the collection and use of personal information" at 32); Sonia K Katyal, "The New Surveillance" 54 Case W Res L Rev 297 at 322; Cohen, "A Right to Read Anonymously", *supra* note 45; Hoofnagle, *supra* note 345; Mulligan, Han & Burstein, *supra* note 32; Kerr & Bailey, *supra* note 60 at 89; Cameron, "DRM: Where Copyright and Privacy Collide", *supra* note 61; Information and Privacy Commissioner/Ontario (IPC), "Privacy and Digital Rights Management (DRM): An Oxymoron?" (October 2002), online: IPC <<http://www.ipc.on.ca/docs/drm.pdf>>; Hayes, *supra* note 64; Helberger et al, "INDICARE 2004", *supra* note 31; Jonathan Weinberg, "Hardware-Based ID, Rights Management, and Trusted Systems" (2000) 52 Stan L Rev 1251. See also Part III of Chapter 1.

³⁵⁸ Helberger et al, "INDICARE 2004", *ibid* at 8.

³⁵⁹ Article 29 Data Protection Working Party, "Working document on data protection issues related to intellectual property rights WP104" (18 January 2005) at 8, online: Europa

Consistent with the Working Party's view, the *EU Copyright Directive*³⁶⁰ codifies recognition that DRM can have an impact on privacy and provides that DRM should be designed in accordance with the *EU Data Protection Directive*.³⁶¹

Recognizing the potential privacy implications of DRM, in 2004 the OPC identified DRM as posing a threat to individuals similar to the threat posed by 'spyware' and RFID technologies.³⁶² This conclusion was borne out in 2005 when Sony-BMG was the subject of a high-profile controversy regarding its Extended Copy Protection (XCP) DRM technology.³⁶³ When an individual inserted a music CD containing the XCP DRM into their Windows computer, the XCP system installed a program in the root system of the computer which was designed to, among other things, prevent copying of the CD. The program was installed secretly, without individuals' knowledge or consent.³⁶⁴

<http://ec.europa.eu/justice_home/fsj/privacy/docs/wpdocs/2005/wp104_en.pdf>.

³⁶⁰ EC, *Directive 2001/29/EC of the European Parliament and of the Council of 22 May 2001 on the harmonisation of certain aspects of copyright and related rights in the information society*, [2001] O.J. L. 167/10 at Art 6, online: Europa <http://europa.eu.int/eur-lex/pri/en/oj/dat/2001/l_167/l_16720010622en00100019.pdf> [*EU Copyright Directive*].

³⁶¹ *EU Data Protection Directive*, *supra* note 204.

³⁶² OPC, January 2008 Letter, *supra* note 56.

³⁶³ See e.g. Mark Russinovich, "Sony, Rootkits and Digital Rights Management Gone Too Far", *Mark's Blog* (31 October 2005), online: Mark Russinovich <<http://blogs.technet.com/markrussinovich/archive/2005/10/31/sony-rootkits-and-digital-rights-management-gone-too-far.aspx>>; Bruce Schneier, "Real Story of the Rogue Rootkit", *Wired.com* (17 November 2005), online: Wired <<http://www.wired.com/politics/security/commentary/securitymatters/2005/11/69601>>; Jeremy DeBeer, "How Restrictive Terms and Technologies Backfired on Sony BMG" (2006) 6 *Internet & E-Commerce Law in Canada* 93 [deBeer, "Backfired"].

³⁶⁴ *Ibid.*

The XCP DRM caused security vulnerabilities in the computers and networks on which it was installed.³⁶⁵ These security concerns led US Computer Emergency Readiness Team, an arm of the National Cyber Security Division at the Department of Homeland Security, to issue a recommendation that individuals not install software from audio CDs.³⁶⁶ Microsoft categorized the XCP DRM as 'spyware'.³⁶⁷ The Texas Attorney General commenced an action against Sony-BMG, alleging, among other things, that the DRM system violated the state's spyware and deceptive trade practices laws.³⁶⁸ Class action lawsuits were launched in Canada.³⁶⁹

The XCP DRM raised significant privacy concerns because when an XCP-enabled CD was played on a computer with an Internet connection, the program opened the computer to potential attack by hackers and viruses. The program could also "phone home"³⁷⁰ to send information to Sony-BMG, including the computer's internet protocol (IP) address, information about when a CD was played

³⁶⁵ *Ibid.*

³⁶⁶ US CERT, "First 4 Internet XCP (Sony DRM) Vulnerabilities" (18 November 2005), online: US CERT <<http://www.us-cert.gov/current/archive/2005/11/21/archive.html#xcpdrm>>.

³⁶⁷ British Broadcasting Corporation (BBC), "Microsoft to remove Sony CD code" *BBC News* (14 November 2005), online: BBC <<http://news.bbc.co.uk/1/hi/technology/4434852.stm>>.

³⁶⁸ Texas Attorney General, Press Release, "Attorney General Abbott Brings First Enforcement Action In Nation Against Sony BMG For Spyware Violations" (21 November 2005), online: OAG <<http://www.oag.state.tx.us/oagnews/release.php?id=1266>>.

³⁶⁹ Canadian class actions were settled. Sony-BMG established a website to provide information regarding the settlements reached: <<http://cdtechsettlement.sonybmga.ca/en/>>. See also Jeremy deBeer, "Sony BMG Settles Canadian Class Actions" (19 November 2006), online: Jeremy deBeer <http://www.jeremydebeer.ca/index.php?option=com_content&task=view&id=87>.

³⁷⁰ Greenleaf, *supra* note 48.

and information about whether the individual had attempted to copy the CD.³⁷¹ The OPC provided the following account of its privacy-related concerns in connection with the XCP DRM:

Failing to give adequate notice that these technologies are being used and failing to obtain informed consent from users;

Automatically installing files even when users choose not to run the application. Although users may be presented with terms and conditions that refer to software installation before launching the CD, it appears safe to assume that few, if any, realize that doing so could result in a security and potential privacy risk;

Requiring users to reveal their identity and rights to access protected content, thus preventing the anonymous consumption of content;

Facilitating the profiling of users' preferences or limiting access to certain content. This is done by assigning an identifier to content or to the content player, and attaching personal information to the identifier. If based on online verification, DRMs may invade people's privacy by tracking personal data and transmitting them to DRM managers;

Establishing a connection with the vendor's site and sending the site an ID associated with the media or content. Vendors may not be doing anything with the data, but with this type of connection their servers

³⁷¹ See e.g. Dan Kaminsky, "Welcome To Planet Sony" (15 November 2005), online: Doxpara <<http://www.doxpara.com/?q=sony>>; deBeer, "Backfired", *supra* note 363 (describing how the DRM technologies at issue "surreptitiously monitor and report information about consumers' computer systems and listening activities" at 98); OPC, "DRM Fact Sheet", *supra* note 57.

could record each time a copy-protected CD is played and the IP address of the computer playing it; and

Failure of the uninstaller programs to completely remove the software.³⁷²

Lest the Sony BMG controversy be considered an isolated incident, it is worth noting that a similar controversy erupted in 1999 when it was learned that RealNetworks embedded an identifier in its RealJukebox software that was capable of linking individuals' listening habits with other personal information, including their home address.³⁷³ Security and privacy questions have also arisen in the use of DRM on DVDs³⁷⁴ and in an early case involving DRM on a music CD.³⁷⁵ The XCP DRM incident is significant, however, because it unquestionably woke the world to the potential privacy implications of DRM in ways that no prior incident had ever done.

In early 2008, the OPC issued a public letter to Industry Canada and Canadian Heritage, the Canadian government ministries responsible for Canadian copyright law, expressing concern about the privacy implications of DRM and citing Sony-BMG XCP DRM as an example.³⁷⁶

³⁷² OPC, "DRM Fact Sheet", *ibid.*

³⁷³ BBC News, "Real sorry after privacy row" *BBC News* (2 November 1999), online: BBC <<http://news.bbc.co.uk/2/hi/science/nature/502925.stm>>.

³⁷⁴ See e.g. Heise Online, "DVD Copy Protection Creates Security Risk", *Heise Online* (14 February 2006), online: Heise Online <<http://www.heise.de/english/newsticker/news/69608>>.

³⁷⁵ See e.g. *DeLise v Fahrenheit*, No CV-014297 (Cal Sup Ct, September 6, 2001) (Plaintiff's complaint), online: TechFirm <<http://www.techfirm.com/mccomp.pdf>>. This case was settled. The settlement can be found at the following website: <<http://www.techfirm.com/sunnk.pdf>>.

³⁷⁶ OPC, January 2008 Letter, *supra* note 56.

Prior to and following the XCP controversy, a number of studies surveyed the use of DRM in the market and considered, among other issues, the privacy implications that DRM can raise. In a groundbreaking study published in 2003, researchers at the University of California at Berkley examined a number of DRM-enabled content delivery systems for music and movies; they concluded that privacy concerns were merited:

[...] The DRM systems we examined engage in detailed surveillance of content consumption by consumers within private spaces. In most instances the systems monitor the content used, the time of use, the frequency of use, and the location of use. The services both limit what consumers can do in the confines of their own home, or the equivalent, and create detailed reports about use of digital works. In addition to monitoring and reporting by the service itself, there are multiple third parties who monitor and collect data about individuals' use of the site. These entities are not well disclosed, and discovering their identities and use of the data requires detailed reading of privacy policies.³⁷⁷

In 2004, the European Commission's INDICARE project – the Informed Dialogue about Consumer Acceptability of DRM Solutions in Europe – issued its first 'state-of-the-art' report on the status of DRM in Europe.³⁷⁸ In a number of areas, this report identified consumer privacy concerns with DRM as well as possible solutions for these concerns.³⁷⁹ The report was followed by a supplement in 2005³⁸⁰ and a “Consumer’s guide to Digital Rights

³⁷⁷ Mulligan, Han & Burstein, *supra* note 32.

³⁷⁸ Helberger et al, “INDICARE 2004”, *supra* note 31.

³⁷⁹ *Ibid* at 22, 85.

³⁸⁰ Helberger et al, “INDICARE 2005”, *supra* note 31.

Management” in 2006,³⁸¹ each of which reinforced the numerous privacy issues that can be raised by DRM.

In 2007, the Canadian Internet Policy and Public Interest Clinic (CIPPIC) conducted a similar study of DRM-enabled content delivery services in use in the Canadian marketplace.³⁸² The DRM-protected works tested in the CIPPIC Study included music on CDs, online music download services, feature films on DVDs, digital e-books, digital audio books, video games, software, and a mobile phone music delivery service.³⁸³ These products and services were subjected to technical testing and assessment and the results were then evaluated against Canadian privacy law. The example of eReader is among the services discussed in detail in the CIPPIC report.³⁸⁴

Researchers in the CIPPIC study concluded, among other things, that a number of DRM systems in use in the Canadian market raised legitimate privacy concerns: “Fundamental privacy-based criticisms of DRM are well-founded: we observed tracking of usage habits, surfing habits, and technical data.”³⁸⁵ The CIPPIC study also found shortcomings in respect of compliance with *PIPEDA*, including a fundamental problem in a number of cases where organizations had inadequate privacy policies in place and did not consider internet protocol addresses to be personal information subject to *PIPEDA*.³⁸⁶

³⁸¹ INDICARE, “Consumer’s guide to Digital Rights Management” (April 2006), online: INDICARE <http://www.indicare.org/tiki-download_file.php?fileId=195>.

³⁸² CIPPIC, “Digital Rights Management and Consumer Privacy”, *supra* note 30.

³⁸³ *Ibid* at i.

³⁸⁴ *Ibid* at 35, 47.

³⁸⁵ *Ibid* at ii.

³⁸⁶ See e.g. *ibid* at ii, iv, v.

A number of the examples described above demonstrate that DRM's privacy implications are not limited to online digital content. The measure of privacy previously afforded by the ownership of tangible goods has eroded in the digital age. Purchasing a physical item such as a CD, DVD, or a video game in a traditional 'bricks-and-mortar' store does not mean that privacy considerations do not arise.³⁸⁷ During playback of these physical media on a computer, or video game console connected to the Internet, for example, information about individuals' access to and use of the work can be collected and transmitted to a copyright holder or other entity in real time or at a later time.³⁸⁸

It is important to note that the potential privacy impact of DRM goes beyond the mere collection and use of information related to individuals' private enjoyment of copyright works; in other words, DRM implicates more than just informational privacy.³⁸⁹ DRM's incursion into the private sphere can constrain and interfere with individuals' intellectual freedom to explore ideas and creative works in conditions of privacy. Cohen describes this effect of DRM as follows:

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.³⁹⁰

³⁸⁷ *Ibid.* See also deBeer, "Backfired", *supra* note 363 (discussing the Song BMG DRM incident involving audio CDs).

³⁸⁸ *Ibid.* See also Napster, *supra* note 354 (describing how information is collected while an individual is offline and is then transmitted to Napster when the individual reconnects to the Internet).

³⁸⁹ This point was also made in Chapter 1 and will be further discussed in Chapter 3.

³⁹⁰ Cohen, "DRM and Privacy" *supra* note 3 at 580.

Cohen asserts that such technologies require us to rethink “the nature of privacy and what counts, or ought to count, as privacy invasion in the age of networked digital technologies.”³⁹¹ In other words, the reduction in individuals’ autonomy in relation to copyright works may be considered a type of privacy violation in addition to DRM’s monitoring and information collection functions.³⁹²

DRM’s privacy impact can also extend beyond just works that are DRM-protected. To the extent that individuals cannot distinguish between works that are protected by DRM and those that are not, they may simply assume that they are being monitored while accessing or enjoying all copyright works or other information.

II. Law

Building on the basic provisions of copyright law, there are a number of related areas of law that bear on the conflict between copyright and privacy: (i) contract law, (ii) anti-circumvention and anti-device laws, (iii) intermediary liability laws and (iv) laws that relate to enforcement of copyright (e.g. file-sharing lawsuits).³⁹³ The

³⁹¹ *Ibid* at 575.

³⁹² This interference with autonomy does not appear to depend on whether the individual is identifiable or not.

³⁹³ There is some question as to whether anti-circumvention and anti-device laws are properly the subject of copyright, leading some to suggest that such provisions are “para-copyright” laws. See e.g. David Nimmer, “Puzzles of the Digital Millennium Copyright Act” (1998-1999) 46 *Journal of the Copyright Society of the USA* 401 at 405; Jeremy F deBeer, “Constitutional Jurisdiction Over Paracopyright Laws” in Geist, *In the Public Interest*, *supra* note 11; Kristin Brown, “Digital Rights Management: Trafficking in technology that can be used to circumvent the intellectual property clause” (2003) 40 *Hous L Rev* 803 at 815.

following sections introduce some of the ways that such laws can create or exacerbate conflict between copyright and privacy.³⁹⁴

A. Contracts and copyright

Copyright holders have long used contracts (i.e. licenses) in order to exploit their works, for example, by licensing different publishers to publish a work.³⁹⁵ Contracts are a fundamental means by which copyright holders and their licensees disseminate and exploit copyright works. Section 3 of the *Copyright Act* provides copyright holders with not only the right to exercise their exclusive rights in relation to works, but also the right to *authorize* others to do so. Copyright holders can exercise the latter right through the use of licenses. Section 13(4) of the *Copyright Act* expands on this notion:

Assignments and licences

(4) The owner of the copyright in any work may assign the right, either wholly or partially, and either generally or subject to limitations relating to territory, medium or sector of the market or other limitations relating to the

³⁹⁴ As discussed in Chapter 5, these laws can sometimes mitigate conflict between copyright and intellectual privacy; indeed, there are strong reasons to believe that such laws are not living up to their potential in that regard.

³⁹⁵ See e.g. Lucie MCR Guibault, *Copyright Limitations and Contracts: An Analysis of the Contractual Overridability of Limitations on Copyright* (London: Kluwer Law International, 2002) at 47 [Guibault, *Copyright Limitations and Contracts*] at 15. The terms “contract” and “license” are used interchangeably in this dissertation. Although the difference between the terms is not relevant for the purposes of this dissertation, it must be acknowledged that the two terms can sometimes denote relationships with different legal consequences. See generally Niva Elkin-Koren, “What Contracts Can't Do: The Limits of Private Ordering in Facilitating a Creative Commons” (2005) 74 *Fordham L Rev* 375. See also Giuseppina D'Agostino, *Copyright, Contract, Creators* (Cheltenham: Edward Elgar, 2010).

scope of the assignment, and either for the whole term of the copyright or for any other part thereof, and may grant any interest in the right by licence, but no assignment or grant is valid unless it is in writing signed by the owner of the right in respect of which the assignment or grant is made, or by the owner's duly authorized agent.

The *Copyright Act* refers to the rights of licensees in a number of areas.³⁹⁶

Contracts that authorize others to engage in activities falling within a copyright holder's exclusive rights often spell out the terms and conditions upon which such authorization is granted. For example, a copyright holder might contract with a movie theatre to permit the theatre to screen a copyright film only between 6pm and 9pm on Thursday nights. The copyright holder might have any number of entirely legitimate motivations for imposing this term. For example, the copyright holder might wish to license more popular theatres to display the film on busier nights of the week. There is nothing in the *Copyright Act* that expressly permits or prohibits a copyright holder from setting the time at which a copyright work will be broadcast to the public; this is merely a specific contractual term under which the copyright holder can choose to permit another entity to do something, (in this case to publicly display a film) that the copyright holder has the exclusive right to do under the *Copyright Act*.³⁹⁷

Copyright holders' tradition of utilizing contracts with distributors, performers, publishers and others in order to derive revenue from the use of copyright works has evolved in the digital age. Digital technologies have opened up new opportunities for copyright holders and others to contract directly *with individuals* in respect of

³⁹⁶ See e.g. *Copyright Act*, *supra* note 2, ss 13(4), 44.1(2.1), 44.3.

³⁹⁷ *Ibid*, s 3.

copyright works. Standard form contracts now commonly accompany copyright works, including “clickwrap” and “browsewrap” license agreements, end user license agreements (EULAs) and other forms of terms and conditions of service.³⁹⁸ These contracts specify the detailed terms and conditions under which individuals are permitted to access and use the works. Such terms and conditions can include the kinds of things that were earlier referenced as being things that DRM might technologically enforce – e.g. ‘read, but don't copy’, ‘read, but don't print’, ‘read, but only copy five times’. Although contracts are not new in copyright, the use of contracts to bind *individuals* and their devices, particularly in respect of very discrete activities, is a novel development in the history of copyright.³⁹⁹

Contracts that regulate individuals' access to and use of works are commonly used for digital works and are often implemented and enforced using DRM technology. Contracts in respect of DRM protected works often include a term that gives the copyright

³⁹⁸ For a general discussion of the differences between these forms of contracts, see Christina L Kunz et al, “Browse-Wrap Agreements: Validity of Implied Assent in Electronic Form Agreements” (2003) 59 *The Bus Lawyer* 291.

³⁹⁹ See generally Garnett, “Automated Rights Management Systems”, *supra* note 39 at 79:

DRM systems [...] give the content provider, through the digital licensing mechanism, control over the functioning of the machine on which the content will be used in relation to the use of that content. Usually, there is no alternative digital licence other than that of the content provider, and without the instructions contained in the digital licence the machine will simply not function in relation to the content in question. In simple terms this might be seen as a record company not only delivering the CD but also the remote control device enabling it to be played.

See also Daniel Gervais, “Use of Copyright Content on the Internet: Considerations on Excludability and Collective Licensing” in Geist, *In the Public Interest*, *supra* note 11 at 523.

holder or other entity the right to monitor individuals' activities. For example, the Terms of Service of MTV's DRM-enabled 'Overdrive' service includes the following provision: "If you are a registered user, you also acknowledge, understand and hereby agree that you are giving us your consent to *track your activities...*"⁴⁰⁰ The terms accompanying Pinnacle Systems' video editing software describes how Pinnacle Systems may automatically monitor an individuals' computer software in order to install updates that may, among other things, disable the ability to play underlying DRM-protected content:

You acknowledge and agree that in order to protect the integrity of certain third party content, Pinnacle and/or its licensors may provide for Software security related updates that will be automatically downloaded and installed on your computer. Such security related updates may impair the Software (and any other software on your computer which specifically depends on the Software) including disabling your ability to copy and/or play "secure" content, i.e. content protected by digital rights management. In such an event, Pinnacle and/or its licensors shall use reasonable efforts to post notices promptly on Pinnacle's web site explaining the security update and providing instructions to end-users for obtaining new versions or further updates of the Software that restore access to secure content and related features.⁴⁰¹

⁴⁰⁰ See MTV's Privacy Policy at <<http://www.mtv.com/overdrive/about/privacy.jhtml>>. MTV's FAQ explains that the Overdrive service is DRM-enabled: <<http://www.mtv.com/overdrive/about/faq.jhtml>>.

⁴⁰¹ Pinnacle Systems Inc, "Pinnacle Studio 9" (2004) at 342-343, online: Pinnacle <[http://www.pinnaclesys.com/WebVideo/Studio%20version%209/English\(US\)/doc/Studio_e.pdf](http://www.pinnaclesys.com/WebVideo/Studio%20version%209/English(US)/doc/Studio_e.pdf)>, cited in Annalee Newitz, "Dangerous Terms: A User's Guide to EULAs" (February 2005), online: EFF <<http://www.eff.org/wp/dangerous-terms-users-guide-eulas>>.

Many contemporary licenses for digital content require individuals to agree to be monitored in one form or another if they wish to have access to creative works. In addition to MTV Overdrive and Pinnacle Systems, similar terms of service for Napster, eReader, Google, Bookshare.org, and Country Music Television were referenced earlier in this dissertation.⁴⁰² There are many other examples of contracts that include similar provisions, as well as provisions that permit organizations to use and share information about individuals' activities in relation to copyright works.⁴⁰³ Kerr notes that organizations can use this combination of technology and contract "as a kind of privacy circumvention device."⁴⁰⁴

Indeed, readers familiar with the usual process of clicking on 'I Agree' in the context of any number of computer-based activities will understand why DRM and contracts can have a profound impact on privacy. If privacy can be waived by clicking 'I Agree' to standard form contracts presented and enforced through DRM, then privacy is at risk of being contracted away without individuals knowing or understanding that they are doing so.⁴⁰⁵ Solove puts the point more generally as follows:

Giving people property rights or default contract rules is not sufficient to remedy the problem because it does not address the underlying power inequalities that govern information transactions. Unless these are addressed, any privacy protections will merely be "contracted" around, in ways not meaningful either to the problem or to the contract notions supposedly

⁴⁰² See Chapter 1 and Part I(C) of this chapter.

⁴⁰³ See Newitz, *supra* note 401. See also CIPPIC, "Digital Rights Management and Consumer Privacy", *supra* note 30; Mulligan, Han & Burstein, *supra* note 32.

⁴⁰⁴ Kerr, "If Left to their own Devices", *supra* note 42 at 170.

⁴⁰⁵ There are also many instances where license language, terms of service, or a privacy policy are not even presented to individuals during the process of accessing or using a copyright work. See generally CIPPIC, "Digital Rights Management and Consumer Privacy", *supra* note 30.

justifying such a solution. People will be given consent forms with vague fine-print discussions of the contractual default privacy rules that they are waiving, and they will sign them without thought.⁴⁰⁶

This 'legal fiction' that individuals consent when they agree to standard form contracts is not unique to DRM or to the copyright context.⁴⁰⁷ Standard form contracts have raised myriad legal and policy concerns since at least the nineteenth century.⁴⁰⁸ Courts have grappled with how traditional contracts principles ought to be applied in the context of mass produced standard form contracts where it is commonly known that, even where such documents are signed, they are often "...signed without being read or understood."⁴⁰⁹ In many cases, the electronic environment reinforces these considerations and raises additional legal and policy questions.⁴¹⁰

⁴⁰⁶ Daniel J Solove, *The Digital Person: Technology and Privacy in the Information Age* (New York: NYU Press, 2004) at 82–85. See also Paul M Schwartz, "Privacy and Democracy in Cyberspace" (1999) 52 Vand L Rev 1609 at 1661.

⁴⁰⁷ Schwartz, *ibid*.

⁴⁰⁸ See e.g. *Parker v South Eastern Railway Co*, [1874–80] All ER Rep 166 (CA) (one of the earliest 'ticket cases' involving the enforceability of terms printed on the back of a baggage claim ticket). See also *Tilden Rent-A-Car Co v Clendenning* (1978), 18 OR (2d) 601 (CA); *Richardson-Watson v 443496 Ontario Inc*, 2005 CanLII 6383 (ON SC); *National Car Rental v Thibodeau*, 2006 NBQB 147. See generally SM Waddams, "Unconscionable Contracts: Competing Perspectives" (1999) 62 Sask L Rev 1.

⁴⁰⁹ *Tilden Rent-A-Car Co v Clendenning*, *ibid* at 408–09. See also Robert L Oakley, "Fairness in Electronic Contracting: Minimum Standards for Non-Negotiated Contracts" (2005) 42 Hous L Rev 1041 ("Clickwrap licenses are ubiquitous today, and most people click to accept without reading the text" at 1051); Robert A Hillman & Jeffrey J Rachlinski, "Standard-Form Contracting in the Electronic Age" (2002) 77 NYU L Rev 429.

⁴¹⁰ See generally Vincent Gautrais, "The Colour of E-consent" (2003–2004) 1 UOLTJ 189 (identifying legibility, speed and other issues unique to individual contracting in the electronic environment and proposing solutions to address these issues); Joseph Savirimuthu, "Online Contract Formation: Taking

If we are to avoid the risk that privacy may be unknowingly contracted away *en masse* if left to the free market, then we must bear in mind, among other things, the principles that have guided courts in past cases involving standard form contracts. In certain circumstances, such contracts may be unconscionable.⁴¹¹ In addition, there are a variety of examples of legislative measures aimed at achieving similar objectives (e.g. consumer protection and other laws that prevent enforcement of terms in consumer contracts wherein consumers purport to waive their rights to participate in class actions, contracts to work for less than minimum wage, etc.) and there appears to be no conceptual reason to suggest that contracts to waive intellectual privacy should be treated differently.⁴¹² For the purpose of understanding copyright's conflict with privacy, however, the principal point of this section is that copyright law does not restrict the use of DRM-enabled standard form contracts that require individuals to agree to be monitored in their access to and use of copyright works. To the extent that copyright law remains silent with respect to the use of standard form contracts to license copyright works directly to individuals, it permits and potentially encourages contractual

Technological Infrastructure Seriously" (2005) 2 UOLTJ 105; Renée Zmurchyk, "Contractual Validity of End User Licence Agreements" (2006) 11 Appeal 55 (noting that end user license agreements often limit individuals' rights in a number of ways at para 15); Kerr, "If Left to their own Devices", *supra* note 42 at 197-99; *Kanitz v Rogers Cable Inc* (2002), 58 OR (3d) 299 (Ont SC); *Rudder v Microsoft Corporation* (1999), 2 CPR (4th) 474 (Ont SC); Carlos Jensen & Colin Potts, "Privacy Policies as Decision-Making Tools: A Usability Evaluation of Online Privacy Notices" in Elizabeth Dykstra-Erickson & Manfred Tscheligi, eds, *Proceedings: ACM Conference on Human Factors in Computing Systems: CHI 2004 Vienna, Austria (April 2004)* 471; Erik Sherman, "Privacy Policies are Great – for PhDs" *BNET* (4 September 2008), online: BNET.com <<http://industry.bnet.com/technology/1000391/privacy-policies-are-great-for-phds/>>.

⁴¹¹ For an American example, see e.g. *Ting v AT&T*, 182 F Supp 2d 902 (ND Cal 2002) at 930.

⁴¹² I am indebted to Jane Bailey for this important point.

practices that can diminish privacy in relation to copyright works, particularly when combined with DRM monitoring.⁴¹³

B. Anti-circumvention and anti-device laws

The second area of law bearing on conflict between copyright and privacy arises in legal provisions called anti-circumvention and anti-device laws. Anti-circumvention and anti-device laws bolster the use of DRM technology by protecting its component parts: TPMs and RMI.

At a conceptual level, it is useful to recognize that anti-circumvention and anti-device laws provide an added layer of protection over copyright works. First, copyright law itself protects copyright works. DRM technologies provide a second layer of protection by endeavouring to control the ways that such works can be accessed and used by individuals. Such DRM practices typically go hand in hand with a third layer of protection: standard form contracts that govern access to and use of works.

On top of the foregoing layers of protection, anti-circumvention laws provide a fourth layer of protection. In general terms, anti-*circumvention* laws prohibit circumvention of technologies that are designed to protect copyright works. As their name suggests, anti-circumvention laws create an actionable wrong for circumventing such technologies.

⁴¹³ Copyright's silence regarding contracts may in part be a result of Canada's particular constitutional structure which relegates jurisdiction over contracting to the provinces, while copyright is a federal matter. Given this constitutional order and the fact that DRM is fundamentally about contracting, some have argued that the federal government may not have constitutional authority to enact anti-circumvention laws. See e.g. deBeer, "Constitutional Jurisdiction Over Paracopyright Laws", *supra* note 393.

Anti-*device* laws provide yet another layer of protection by requiring, to use the *DMCA* as an example, that “[n]o person shall manufacture, import, offer to the public, provide, or otherwise traffic in any technology, product, service, device, component, or part thereof” that is primarily designed to circumvent TPMs.⁴¹⁴

Anti-circumvention and anti-device provisions have been passed into law in a number of countries through ratification of the WIPO Treaties. The WIPO Treaties require the laws of contracting countries to include a form of protection for TPMs. Article 11 of the WCT provides as follows:

Contracting Parties shall provide adequate legal protection and effective legal remedies against the circumvention of effective technological measures that are used by authors in connection with the exercise of their rights under this Treaty or the Berne Convention and that restrict acts, in respect of their works, which are not authorized by the authors concerned or permitted by law.⁴¹⁵

Article 18 of the WPPT contains a similar requirement in connection with TPMs used by performers and producers of phonograms. In addition, Article 12 of the WCT prohibits the removal of RMI from works and the trafficking in works knowing that RMI has been removed.⁴¹⁶

⁴¹⁴ *DMCA*, *supra* note 330, § 1201(2).

⁴¹⁵ WCT, *supra* note 3 at art 12.

⁴¹⁶ Some commentators have considered whether individuals' personal information might itself be included in the definition of RMI in some national laws, thereby meaning that individuals would not have the right to remove their personal information from the work licensed to them. See e.g. Greenleaf, “IP, Phone Home”, *supra* note 48; Bygrave & Koelman, “Privacy, Data Protection and Copyright,” *supra* note 61.

Contracting countries that have ratified the WIPO Treaties in their national laws have taken different approaches.⁴¹⁷ The most widely known example of an anti-circumvention and anti-device law is the United States' *Digital Millennium Copyright Act of 1998*.⁴¹⁸ In general terms, the *DMCA* makes it illegal to circumvent TPMs that effectively control *access* to copyright works, to remove or alter RMI attached to works, and to make any device primarily intended to circumvent TPMs that protect the *right* of a copyright holder in a work.⁴¹⁹ The *DMCA* thus includes anti-circumvention provisions and anti-device provisions.

Canada does not currently have an anti-circumvention or anti-device law in place. Although legislative proposals have been introduced in the past, they have proved highly divisive and controversial and some have questioned whether they are needed at all.⁴²⁰

⁴¹⁷ For a discussion of approaches in different countries, see Michael Geist, "Anti-Circumvention Legislation and Competition Policy: Defining a Canadian Way", in Geist, *In the Public Interest*, *supra* note 11; Mihály Ficsor, *The Law of Copyright and the Internet: The 1996 WIPO Treaties, Their Interpretation and Implementation* (New York: Oxford University Press, 2002); de Werra, *supra* note 9; Pamela Samuelson, "Intellectual Property and the Digital Economy: Why the Anti-Circumvention Regulations Need to Be Revised" (1999) 14 *Berkeley Tech LJ* 519.

⁴¹⁸ *DMCA*, *supra* note 330.

⁴¹⁹ The *DMCA*'s access control protection deals with individual acts of circumvention whereas the rights control (e.g. copy control) protection addresses the manufacture of devices designed to circumvent TPMs. For a discussion of this distinction, see *Coupons, Inc v Stottlemire*, Case No CV 07-03457, (July 2, 2008).

⁴²⁰ Bill C-60, *An Act to amend the Copyright Act*, 1st Sess, 38th Parl, 2005 [Bill C-60]; Bill C-61, *An Act to amend the Copyright Act*, 2nd Sess, 39th Parl, 2008 [Bill C-61]. As a result of intervening elections in Canada, neither Bill C-60 nor Bill C-61 were passed into law. See also Chapter 5, which discusses the more recent manifestations of these proposed amendments. Canadians were divided in support for the proposed laws. See e.g. Angus Reid Strategies, Press Release, "Canadians Evenly Split on Proposed Amendments to

At first glance, one might ask how an anti-circumvention or anti-device law would bear on copyright's conflict with privacy. Such laws do not mandate the use of TPMs and RMI. Nor do such laws specifically contemplate invasions of privacy in the name of protecting copyright works. Anti-circumvention and anti-device laws simply protect TPMs and RMI in the event that such components are used in association with copyright works. Nevertheless, there are at least three ways that anti-circumvention and anti-device laws might contribute to conflict between copyright and privacy.

First, it is possible that providing legal protection to TPMs and RMI may contribute to more widespread use of such technology, including DRMs. If we accept that many forms of DRM currently in use have the effect of diminishing privacy (as described earlier in this chapter) then it follows that anti-circumvention and anti-device laws may thus indirectly contribute to more widespread diminishment of privacy to the extent that they contribute to increased use of privacy invasive DRM in the market.⁴²¹ That said,

Copyright Act" (19 June 2008) (poll finding 45% of Canadians in favour of Bill C-61 and 45% against the bill); Peter Nowak, "Copyright law could result in police state: critics" *CBC News* (12 June 2008), online: CBC <<http://www.cbc.ca/technology/story/2008/06/12/tech-copyright.html>>; Canadian Newspaper Association, "The Impact on Newspapers of Bill C-61, an Act to amend the Copyright Act" (19 June 2008), online: CNA <<http://www.cna-acj.ca/en/news/public-affairs/the-impact-newspapers-bill-c-61-act-amend-copyright-act>>. See also Michael Geist, "Canadian Digital Music Sales Growth Beats The U.S. For Third Consecutive Year" (7 January 2009), online: <<http://www.michaelgeist.ca/content/view/3601/125/>> (reporting that growth in digital music sales in Canada, a country without anti-circumvention or anti-device laws, has exceeded growth in the United States, a country with such laws, for three straight years); Michael Geist, "The music industry's digital reversal" *Toronto Star* (12 January 2009), online: TheStar.com <<http://www.thestar.com/sciencetech/article/569203>>.

⁴²¹ See e.g. Peter K Yu, "Anticircumvention and Anti-Anticircumvention" (2006) 84 *Denv UL Rev* 13 [Yu, "Anticircumvention"] (suggesting, among other

it must be acknowledged that even in countries, including the United States, where DRM is legally protected, there is evidence that many companies may be moving away from DRM because of consumer dissatisfaction with DRM restrictions and interoperability issues, among other factors.⁴²²

Second, providing legal protection for TPMs and RMI may have the effect of legitimizing the use of such technologies from the perspective of potential challenges to DRM under privacy laws of general application as discussed in Chapter 5. In other words, if TPMs and RMI are protected under an anti-circumvention or anti-device provision, it is conceivable that privacy-based challenges to practices involving DRM may be less likely to be successful. After all, if one of the fundamental elements of many current forms of DRM operation is a diminishment of privacy, then the fact that its component parts are protected under an anti-circumvention or anti-device provision might suggest that our legislators have accepted that DRM draws an appropriate balance between the rights of copyright holders and the privacy of individuals.⁴²³ At the very least, if elements of DRM were protected by anti-circumvention or anti-device laws, then that protection would support an argument that such measures are reasonable for the purposes of compliance with data protection legislation⁴²⁴ or that

things, that "... by protecting DRMs, the DMCA has undermined the protection of privacy of individual users" at 39).

⁴²² There are indications that DRM has been dropped in a number of industry sectors in countries, including the United States, that provide legal protection for DRM components. See *supra* note 50 and accompanying text.

⁴²³ It is important to note that some anti-circumvention provisions permit certain acts of circumvention for the purpose of protecting personal privacy. See e.g. *DMCA*, *supra* note 330 at § 1201(i).

⁴²⁴ Reasonableness is one of the requirements of *PIPEDA*. *PIPEDA*, *supra* note 13 s 5(3). For further discussion of the requirements of *PIPEDA* as applied to DRM practices, see Chapter 5.

individuals do not have a reasonable expectation of intellectual privacy in relation to such technologies.

Third, anti-circumvention laws that target the circumvention acts of individuals have the potential to encourage the close monitoring of individuals' behaviours not just to track how they access and use copyright works to ensure that they do so in authorized ways, but also to determine whether they commit or attempt to commit an act of circumvention. For this reason, some commentators have advanced privacy-based arguments in favour of adopting anti-device provisions over anti-circumvention provisions.⁴²⁵ The argument goes that enforcing an anti-device provision protects privacy because it focuses on device-makers and does not necessitate monitoring of individuals' activities as would be needed in the case of anti-circumvention provisions.⁴²⁶ Of course, such arguments do not directly account for the underlying intellectual privacy impacts of DRM monitoring itself and the potential that a prohibition against circumvention devices might eviscerate individuals' practical ability to circumvent a TPM in order to, for example, protect their intellectual privacy as they are entitled to do under some laws.⁴²⁷

Notwithstanding the potentially adverse impacts that anti-circumvention and anti-device laws can have on intellectual privacy as described in this section, it is important to acknowledge that some anti-circumvention laws implicitly acknowledge the privacy threats that DRM monitoring can pose and include

⁴²⁵ See e.g. Ann Chaitovitz, US Patent and Trademark Office, "The Digital Rights Management Dilemma" (Presentation delivered at Musical Myopia, Digital Dystopia: New Media and Copyright Reform, March 23, 2007, McGill Centre for Intellectual Property Policy, Montreal, (video archive), online: McGill Centre for Intellectual Property Policy <<http://www.cipp.mcgill.ca/en/news/newsletter/89/>> at 44:30 – 44:50.

⁴²⁶ *Ibid.*

⁴²⁷ See e.g. *DMCA*, *supra* note 330, § 1201(i).

exceptions that permit circumvention in particular circumstances, including protecting an individual's intellectual privacy.⁴²⁸ Similar privacy countermeasures have been the subject of proposals aimed at balancing privacy interests against the threats posed by DRM and anti-circumvention laws.⁴²⁹ Such countermeasures will be considered in Chapter 5 as potential components of accounting for intellectual privacy within copyright.

C. Internet service provider (ISP) liability

A third area of law that can contribute to conflict between copyright and privacy is ISP liability law.⁴³⁰ Such provisions typically spell out the responsibilities of ISPs to take action in respect of alleged copyright infringement, as well as their associated liabilities for failing to take action.⁴³¹ Although ISP

⁴²⁸ *Ibid.* Bill C-61 would have introduced a similar provision in Canada. See Bill C-61, *supra* note 420 at s 41.14. See also Chapter 5.

⁴²⁹ See e.g. Kerr, "If Left to their own Devices", *supra* note 42.

⁴³⁰ For a general discussion of ISP liability, see Andrew Bernstein & Rima Ramchandani, "Don't Shoot the Messenger! A Discussion of ISP Liability" (2002) 1 CJLT 77; Scott Nesbitt, "Rescuing the Balance? An Assessment of Canada's Proposal to Limit ISP Liability for Online Copyright Infringement" (2003) 2 CJLT 115. Although this section focuses only on the copyright context, the liability of ISPs and other intermediaries for the wide variety of online activities of individuals and others was one of the earliest areas of law to develop in the digital age. See e.g. *Cubby v CompuServe*, (1991) 766 F Supp 135 (SD NY, 1991); *Stratton Oakmont, Inc v Prodigy Services Co*, 1995 WL 323710 (NY Sup Ct 1995).

⁴³¹ For a discussion of the liability of ISPs in the European Union, see Cyril van der Net, "Civil Liability of Internet providers following the Directive on Electronic Commerce" in H Snijders & S Weatherill, *Ecommerce Law* (Hague: Kluwer, 2003) at 53. See also, *EU Copyright Directive*, *supra* note 361 at art 5(1) which includes as an exemption from the exclusive right of reproduction of the author, "temporary acts of reproduction which are transient or incidental and part of a technological process whose sole purpose is to enable (a) a transmission in a network between third parties by an intermediary and (b) a lawful use of a work or other protected material."

liability provisions do not yet form part of the legal landscape in Canada, such laws can include a number of components that can implicate privacy.

One kind of ISP liability provision is a 'notice-and-notice' provision.⁴³² Under such a system, copyright holders can issue notices to be sent to individuals who are alleged to have committed copyright infringement. ISPs must forward such notices to the relevant subscriber(s). ISPs may also be required to retain identifying information about individuals that are sent such notices, perhaps for a limited time period. If the copyright holder commences a lawsuit within the allotted time, then the ISP would have to retain the identity data for a longer period.

Under such a system, privacy issues can arise in respect of the nature of information retained, as well as the length of time that it is retained.⁴³³ For example, the OPC has expressed concern about the impact that ISP liability provisions can have on individuals' privacy interests, noting that a 'notice and notice' provision proposed in Canada raised important privacy concerns:

⁴³² A 'notice and notice' system was proposed first in Bill C-60 and then again in Bill C-61. Bill C-60, *supra* note 420; Bill C-61, *supra* note 420, s 41.26. Each of the elements of a 'notice and notice' system described in this paragraph reflect elements of the proposal in Bill C-61. See also Chapter 5.

⁴³³ In reliance on the evidence of the ISPs, in *BMG v. Doe*, *supra* note 59 at para 43 the Federal Court of Appeal stated that applications for the compelled disclosure of ISP customers' identities must be brought without delay since delay may increase the likelihood of error in the identification process:

If there is a lengthy delay between the time the request for the identities is made by the plaintiffs and the time the plaintiffs collect their information, there is a risk that the information as to identity may be inaccurate. [...] Thus the greatest care should be taken to avoid delay between the investigation and the request for information. Failure to take such care might well justify a court in refusing to make a disclosure order.

[Previously proposed notice and notice] provisions would have allowed copyright holders to send written notice to Internet Service Providers (ISPs), informing them of alleged copyright violators on their network. The network operators would then be required to forward the notice to the alleged copyright violator and to retain records on network use for periods of up to a year while investigation of violations or court action took place. Failure to retain these records would have enabled rights holders to seek damages against the ISP of up to \$10,000.

Allowing a private sector organization to require an ISP to retain personal information is a precedent-setting provision that would seriously weaken privacy protections. When this provision was proposed in a previous proposal to amend the legislation it did not include any threshold that had to be met before the notice could be issued, nor did it provide any means for the ISP to contest the demand to retain the data. The extended retention periods create additional privacy concerns. *PIPEDA* requires that organizations retain personal information for only as long as necessary to fulfill the purposes for which the information was originally collected. Limiting the extent of data collection and period of retention is a key strategy to minimize the risk of data breaches of personal information.⁴³⁴

⁴³⁴ OPC, January 2008 Letter, *supra* note 56. Of course, it must be observed that threatening or actually commencing a legal proceeding can effectively force an organization to retain information or face civil consequences (e.g. spoliation), even though there may be some doubt about whether a tort claim for spoliation could be brought against a third party (such as an ISP) which arguably has no direct duty to preserve information. See generally Jane Bailey, “The Substance of Procedure: Non-Party Disclosure in the Canadian and U.S. Online Music Sharing Litigation” (2006) 43 *Alta L Rev* 615 [Bailey, “The Substance of Procedure”].

Other forms of ISP liability provisions include 'notice and takedown' and 'notice and termination' provisions. Following notice to the affected ISP customer, such regimes can require ISPs to take down individuals' content, block their communications or even terminate their Internet access when a copyright holder issues an allegation of infringement to an ISP. The *DMCA*, for example, contains a notice and takedown regime.⁴³⁵ This regime absolves ISPs of liability when taking down content in accordance with the provisions of the *DMCA*. Notably, the *DMCA* expressly provides that nothing in the law requires ISPs to monitor their customers, a provision which was expressly designed to protect the privacy of Internet users.⁴³⁶

Forms of 'notice and termination' provisions for repeat copyright infringers have been considered in England⁴³⁷, rejected in Germany⁴³⁸, Sweden⁴³⁹, and in New Zealand.⁴⁴⁰ Further, under a

⁴³⁵ *DMCA*, *supra* note 330 at § 202. For a critical empirical analysis of notices sent under the *DMCA*, see Jennifer Urban & Laura Quilter, "Efficient Process or Chilling Effects - Takedown Notices under Section 512 of the Digital Millennium Copyright Act" (2005-2006) 22 Santa Clara Computer & High Tech LJ 621.

⁴³⁶ *DMCA*, *supra* note 330 ("[n]othing in this section shall be construed to condition the applicability of subsections (a) through (d) on . . . a service provider monitoring its service or affirmatively seeking facts indicating infringing activity" at § 512(m)). See also HR Rep No 105-551, Part 2, at 64 ("[Section 512(m)] is designed to protect the privacy of Internet users.").

⁴³⁷ See BBC, "Illegal downloaders 'face UK ban'" *BBC News* (12 February 2008), online: BBC <<http://news.bbc.co.uk/2/hi/business/7240234.stm>>; Dugie Standeford, "UK Content, ISP Industries Agree To Partner Against Digital Piracy" *Intellectual Property Watch* (28 July 2008), online: IP Watch <<http://www.ip-watch.org/weblog/2008/07/28/uk-content-isp-industries-agree-to-partner-against-digital-piracy/>>.

⁴³⁸ Wolfgang Spahr, "Germany Rejects Three-Strikes Piracy Plan" *Billboard.biz* (10 February 2009), online: Billboard <http://www.billboard.biz/bbbiz/content_display/industry/e3i73b3660e2c6025e6507555e3cfec977d>.

settlement agreement with four major record labels – EMI, Sony, Universal and Warner – an Irish ISP agreed that it would terminate repeat infringers under a “three strikes and you are out” policy.⁴⁴¹ The terms of this novel agreement also provide that the labels must take “‘all necessary steps’ to put similar agreements in place with all other internet service providers (ISPs) in Ireland.”⁴⁴² This agreement is notable because it is a private agreement independent of any specific legal rule that compels the ISPs to terminate repeat infringers. In Canada, the Canadian Recording Industry Association (CRIA) (now called Music Canada) has in the past asked Canadian law-makers for a notice and termination system in respect of individuals engaged in peer-to-peer file sharing of thousands of songs: “[CRIA] recommend[s] that if [it] find[s] out

⁴³⁹ Andres Guadamuz, “ISP police, Sweden says no” *TechnoLlama* (17 March 2008), online: TechnoLlama <<http://technollama.blogspot.com/2008/03/isp-police-sweden-says-no.html>>.

⁴⁴⁰ New Zealand initially introduced such a law—New Zealand, *Copyright (New Technologies) Amendment Act 2008 No 27*, s 92A—and later withdrew it following widespread controversy and protest. See generally EFF, “New Zealand Goes All Black Against Three Strikes” (17 February 2009), online: EFF <<http://www.eff.org/deeplinks/2009/02/new-zealand-goes-all-black-against-three-strikes>>; 3 News, “Government delays introduction of controversial ‘S92A’” *3 News* (23 February 2009), 3News online: <<http://www.3news.co.nz/Government-delays-introduction-of-controversial-S92A/tabid/412/articleID/92441/cat/73/Default.aspx>>; Chris Keall, “Section 92A to be scrapped” *The National Business Review* (March 23, 2009), online: National Business Review <<http://www.nbr.co.nz/article/section-92a-be-scrapped-89121>>. See also, Michael Geist, “European Parliament Rejects Three Strikes and You’re Out Approach” (26 March 2009), online: MichaelGeist.ca <<http://www.michaelgeist.ca/content/view/3779/125/>>.

⁴⁴¹ John Collins & Mary Carolan, “Internet users face shutdown over illegal music downloads” *Irish Times* (29 January 2009), online: Irish Times <<http://www.irishtimes.com/newspaper/frontpage/2009/0129/1232923373331.html>>.

⁴⁴² *Ibid.*

about this and send[s] a notice to the ISP that this is happening, the ISP ought to kick that subscriber off the system.”⁴⁴³

Extra-judicial copyright enforcement regimes such as ‘notice and takedown’ and ‘notice and termination,’ if adopted, could conflict with individuals’ privacy interests in obvious ways, particularly if ISPs are required to retain data on their customers in respect of such notices.⁴⁴⁴ Among other impacts, an effective notice and termination regime, for example, would presumably involve linking an individual’s identity and subscriber information to a notice and termination history so that the same individual could not re-apply for ISP service with the same ISP. It is also conceivable that ISPs might share such information with one another in order to avoid ‘problem’ customers. Termination can also have broader social welfare costs as identified in Sweden’s rejection of a notice and termination system:

The proposal in the Renfors-review that ISPs should be given the right and be forced to shut down subscribers whose Internet subscription has repeatedly been used for infringing copyrights has met with strong criticism. Many have noted that shutting down an Internet subscription is a wide-reaching measure that could have serious repercussions in a society where access to

⁴⁴³ Richard Pfhof, Canadian Recording Industry Association, (Testimony delivered at the Standing Committee on Canadian Heritage, April 22, 2004), online: Parliament of Canada <<http://www.parl.gc.ca/committee/CommitteePublication.aspx?SourceId=80792>>.

⁴⁴⁴ See generally EFF, “Unsafe Harbors: Abusive DMCA Subpoenas and Takedown Demands”, (September 2003), online: EFF <<http://www.eff.org/wp/unsafe-harbors-abusive-dmca-subpeonas-and-takedown-demands>> (“The DMCA has been used to invade the privacy of Internet users, harass Internet service providers, and chill online speech. The subpoena and takedown powers of Section 512 are not limited to cases of proven copyright infringement, and are exercised without a judge’s review”); OPC, January 2008 Letter, *supra* note 56.

the Internet is an imperative welfare-issue. The government has, because of this, decided not to pursue this proposal.⁴⁴⁵

In each of the notice and termination provisions identified in this section, the concept of a 'repeat infringer' is central. Some commentators suggest that such language must require a showing *in court* that the individual engaged in infringement on multiple occasions, despite warnings.⁴⁴⁶ However, there is often ambiguity in such language, leaving open an interpretation that ISPs must terminate individuals who have been merely accused of infringement on multiple occasions.⁴⁴⁷

In addition to requirements imposed on ISPs by law, it is important to bear in mind the potential incentives that ISPs and other intermediaries may have, independent from legal requirements, that could lead them to monitor individuals' access to and use of copyright works. For example, information about individuals' searches for, access to and use of copyright works may be valuable to an ISP that wishes to advertise to its customers or that wishes to permit others to advertise to its customers. These additional market-based considerations are applicable to ISPs and to a wide range of other potential intermediaries in the copyright distribution chain as discussed below in this chapter.

⁴⁴⁵ Reported in Guadamuz, *supra* note 439.

⁴⁴⁶ David Nimmer, "Repeat Infringers" (2005) 52 J Copyright Soc'y (discussing the notice and termination provision of the DMCA). Nimmer points out that most motion picture studios would be barred from Internet access because they have been found guilty of infringement in the courts on multiple occasions.

⁴⁴⁷ For a description of the consequences that can follow from this interpretation, as reflected in actual cases, see Wendy Seltzer, "DMCA 'Repeat Infringers': Scientology Critic's Account Reinstated after Counter-Notification" *Chilling Effects* (6 June 2008), online: Chilling Effects <<http://www.chillingeffects.org/weather.cgi?WeatherID=605>>.

D. Copyright litigation

Peer-to-peer file-sharing of music, movies and software, as well as posting of copyright works on websites and blogs and in discussion forums, among other activities, have all spawned a plethora of copyright litigation in the digital age. In many cases, this litigation pits individuals' privacy interests directly against the interests of copyright holders that wish to pursue legal claims for copyright infringement. Thus, in addition to contract law and the statutory provisions discussed in the preceding sections, certain aspects of copyright enforcement law can have important implications for privacy.

Peer-to-peer file sharing litigation was first directed against the operators of peer-to-peer networks, including the original Napster file-sharing service.⁴⁴⁸ Subsequent legal action has been brought against entities that provide software or otherwise facilitate peer-to-peer file sharing.⁴⁴⁹ Yet, because peer-to-peer providers do not typically collect or retain information about individuals that use their products or services, litigation against such entities has to-date not directly given rise to conflict with individuals' privacy interests.⁴⁵⁰

In addition to suits against peer-to-peer software and service providers, copyright litigation has been brought against individuals who are alleged to have committed copyright infringement by sharing copyright works on peer-to-peer networks.

⁴⁴⁸ *A&M Records, Inc v Napster, Inc*, *supra* note 26.

⁴⁴⁹ See e.g. *MGM Studios, Inc. v Grokster, Ltd.*, 545 US 913 (2005).

⁴⁵⁰ It must be acknowledged, however, that litigation against peer-to-peer file sharing services can eliminate a means by which individuals can efficiently share copyright works and other information in conditions of intellectual privacy. This benefit is unfortunately overshadowed by the fact that peer-to-peer systems are used by many as a means to share copyright works in violation of copyright law.

Tens of thousands of such lawsuits have been brought against individuals all around the world.⁴⁵¹ Copyright holders investigating such cases are typically in possession of only an IP address belonging to a targeted ISP subscriber, a list of files being shared, and the time that the individual was alleged to have been sharing the files.⁴⁵² Using this information, copyright holders that wish to bring an action against a targeted individual can usually only obtain information about the identity of the individual from the relevant ISP, often only pursuant to a court order. This is because peer-to-peer file-sharing systems typically allow individuals to participate in a file-sharing network without revealing their identity to either the peer-to-peer software or service provider or to other individuals on the network.⁴⁵³ Individuals are typically able

⁴⁵¹ For an updated index of peer-to-peer copyright infringement litigation documents in the United States, see Ray Beckerman, "Recording Industry vs. The People" online: Recording Industry vs. The People <<http://recordingindustryvspeople.blogspot.com/2007/01/index-of-litigation-documents.html>>. See also Eric Bangeman, "IFPI files 8,000 new file-sharing lawsuits" *Ars Technica* (17 October 2006), online: Ars Technica <<http://arstechnica.com/news.ars/post/20061017-8001.html>>.

⁴⁵² Similar forms of information might be available in a case where an individual posted a copyright work on a website forum.

⁴⁵³ See generally Kerr & Cameron, "Nymity, P2P & ISPs", *supra* note 59. For a more technical description of a number of 'anonymous' peer to peer systems, see Tom Chothia & Konstantinos Chatzikokolakis, "A Survey of Anonymous Peer-to-Peer File-Sharing" in Tomoya Enokido, ed, *Embedded and Ubiquitous Computing* (Berlin: Springer, 2005) 744. In some cases where peer-to-peer software providers have offered an advertisement-free program to individuals for a fee, individuals have been required to register for the service and provide payment information, such as a credit card number. It is thus conceivable that peer-to-peer providers may in some cases hold varying degrees of personal information about the individuals that use their software or services. Although there appear to have been no reported instances where a peer-to-peer provider has been compelled to disclose information about the individuals that use their service, it is important to note that peer-to-peer providers, like any intermediary, could be compelled to disclose information about individuals' activities in respect of copyright works. For example, Limewire, a peer to peer software provider, indicates that it logs individuals'

to create one or more pseudonyms and to share files through their pseudonym.

The question of whether a court will order an ISP or other intermediary to disclose information about an individual's identity is often dependent on privacy considerations. This places the spotlight on the procedure, or the test, which must be followed before ISPs are compelled to reveal the identity of individual subscribers. Not surprisingly, laws and procedures for obtaining the identity of the targeted subscriber vary by country.⁴⁵⁴

Canada's only case to-date addressing the compelled disclosure of identity in a file-sharing case is *BMG v Doe*,⁴⁵⁵ a 2005 decision of the Federal Court of Appeal. In this case, the court had to decide whether to order five Canadian ISPs to disclose to CRIA the identity of 29 subscribers alleged to have committed copyright infringement on peer-to-peer networks.

In *BMG v. Doe*, the lower court refused to order disclosure. Critical of the plaintiffs' evidence in support of the request for disclosure, the lower court ruled that privacy considerations in the case outweighed the public interest in permitting the copyright holders to pursue their infringement lawsuits:

IP addresses, although it claims not to link them to any personally identifiable information. Limewire, "Privacy Policy", online: Limewire <<http://www.limewire.com/about/privacy.php>>.

⁴⁵⁴ See generally Melody Yiu, "A new prescription for disclosure: reformulating the rules for the Norwich order" (2007) 65 UT Fac L Rev 41. For a comparative review of compelled disclosure of identity of confidential sources in the news context, see Janice Brabyn, "Protection Against Judicially Compelled Disclosure of the Identity of News Gatherers' Confidential Sources in Common Law Jurisdictions" (2006) 69 Modern Law Review 895. See also *Sony Music Entertainment v Does 1-40*, 326 F Supp 2d 556 (SDNY, 2004).

⁴⁵⁵ *BMG v Doe*, *supra* note 59.

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.⁴⁵⁶

The lower court also acknowledged that the individual ISP subscriber may not be the individual who actually engaged in the file sharing.⁴⁵⁷ For example, an individual might hold an ISP subscription for their entire household (including roommates or family members) or for an organization. It is also possible that a wireless Internet connection or local area network could be used by any number of persons, not the subscriber, to share files.

Despite these findings, the lower court made clear that privacy would not always win the day when it came into conflict with copyright. The plaintiff copyright holders in *BMG v Doe* were given the option of returning to court with better evidence of the alleged wrongdoing, including reliable evidence of the link between the IP addresses and the peer-to-peer pseudonyms at issue. Had they

⁴⁵⁶ *BMG Canada Inc v John Doe*, 2004 FC 488 [*BMG v Doe (FC)*] at para 42.

⁴⁵⁷ See *BMG v Doe (FC)*, *ibid* at para 34:

[A]t best the ISPs will generate the name of the account holders; however, they can never generate the name of the actual computer users. An IP address, for instance, can lead to the name of an account holder, but that account holder could be an institution and/or may be linked to a local area network of many users.

done so, the court would likely have ordered disclosure of the individuals' identities, albeit with confidentiality protections built into the disclosure order so that individuals' identities would not be made public right away.⁴⁵⁸ In this way, the court sought to balance individuals' privacy interests against the plaintiffs' interest in pursuing their legal claims.

On appeal, the Federal Court of Appeal agreed with the lower court's evidentiary criticisms and refused to order disclosure of identity information:

Much of the crucial evidence submitted by the plaintiffs was hearsay and no grounds are provided for accepting that hearsay evidence. In particular, the evidence purporting to connect the pseudonyms with the IP addresses was hearsay thus creating the risk that innocent persons might have their privacy invaded and also be named as defendants where it is not warranted. Without this evidence there is no basis upon which the motion can be granted and for this reason alone the appeal should be dismissed.⁴⁵⁹

The appeals court also noted that privacy must be invaded in the "most minimal way" in such cases.⁴⁶⁰ For the court, this included a requirement that:

⁴⁵⁸ *BMG v Doe (FC)*, *ibid* at para 42.

⁴⁵⁹ *BMG v Doe*, *supra* note 59 at para 21. A similar outcome was reached in the United States in *London-Sire Records v Does 1-4* where the court refused disclosure out of concern for the potential that innocent persons would be exposed to lawsuits. See *London-Sire Records v Does 1-4* (2008) D Mass, No 1:04-cv-12434. For a discussion of this decision, see Jamie Wicks, "Judge Quashes Recording Industry Subpoena Seeking the Identities of Three Boston University 'John Does'" *Harvard Journal of Law and Technology Digest* (29 November 2008), online: JOLT Digest <<http://jolt.law.harvard.edu/digest/copyright/london-sire-records-v-does-1-4>>.

⁴⁶⁰ *BMG v Doe*, *supra* note 59 at paras 42-45.

...plaintiffs should be careful not to extract private information unrelated to copyright infringement, in their investigation. If private information irrelevant to the copyright issues is extracted, and disclosure of the user's identity is made, the recipient of the information may then be in possession of highly confidential information about the user. ... Thus in situations where the plaintiffs have failed in their investigation to limit the acquisition of information to the copyright infringement issues, a court might well be justified in declining to grant an order for disclosure of the user's identity.⁴⁶¹

In other countries where similar investigations have not been limited as described above, investigating bodies have been sanctioned for violations of privacy.⁴⁶² Indeed, there is no question that privacy-based limits are finding their way into litigation more generally, with the result that parties and counsel must often consider whether their collection, use and disclosure of information for litigation purposes might run afoul of common law privacy rules or data protection laws.⁴⁶³

⁴⁶¹ *Ibid* at para. 44.

⁴⁶² See e.g. Jeremy Kirk, "Antipiracy group's tactics violate Swiss law" *IDG News Service* (January 2008), online: InfoWorld <http://www.infoworld.com/archives/emailPrint.jsp?R=printThis&A=/article/08/01/25/Antipiracy-group-tactics-violate-Swiss-law_1.html>. See also Winston Maxwell, "Privacy v. Anti-Piracy: Content Owners Warned to Supervise Anti-Piracy Monitor to Ensure Privacy" *Hogan Lovells* (9 July 2011), online: Hogan Lovells <<http://www.hldataprotection.com/2011/07/articles/international-eu-privacy/privacy-v-antipiracy-content-owners-warned-to-supervise-antipiracy-monitor-to-ensure-privacy/>> ("The anti-piracy efforts of the content industry in France recently resulted in a warning from French authorities that, when policing online piracy through use of a third-party contractor, privacy must be respected and enforced").

⁴⁶³ See generally Cameron & Teehan, *supra* note 162; Alex Cameron & Heather Michel, "Obtaining Evidence from Social Media Services and Other Non-Parties", (Paper delivered at the Canadian Association of Counsel to

Finally, the appeals court in *BMG v Doe* made clear that plaintiffs must not delay in bringing their motion to court for disclosure of individuals' identities, since delay can increase the risk of error in the identification process at the ISPs.⁴⁶⁴

BMG v Doe and the thousands of file-sharing lawsuits like it around the world provide examples of a direct tension between copyright and privacy interests.⁴⁶⁵ The legal test for disclosure developed by the courts in such cases represents an attempt by the courts to balance individuals' privacy interests against the need to permit copyright holders to pursue legitimate claims of infringement of their rights.⁴⁶⁶ The precedent-setting test to emerge from *BMG v Doe* is as follows:

(a) the applicant must establish [a *bona fide* claim, i.e. that they really do intend to bring an action for infringement of copyright based upon the information they obtain, and that there is no other improper purpose for seeking the identity of these persons],⁴⁶⁷

Employers 8th Annual Conference, Niagara Falls, 2011); Alex Cameron, "Privacy Issues in Litigation and e-Discovery" (Interview for Nymity's Interviews with Experts, September 2008), online: Nymity <<http://www.nymity.com>>.

⁴⁶⁴ *BMG v Doe*, *supra* note 59 at para 43.

⁴⁶⁵ *Ibid* ("...this case illustrates the tension existing between privacy rights of those who use the Internet and those whose rights may be infringed or abused by anonymous Internet users" at para 1).

⁴⁶⁶ This balancing is designed to ensure that innocent individuals are not exposed to lawsuits. The test also balances the interests of the third party ISPs that have obligations to their customers under privacy laws and that seek compensation for their costs incurred in identifying individuals. See *ibid* ("...if an order for disclosure were granted, consideration would have to be given to the costs incurred by the [ISPs] in assembling the information" at para 35).

⁴⁶⁷ *Ibid* at para 34.

- (b) the person from whom discovery is sought must be in some way involved in the matter under dispute, he must be more than an innocent bystander;
- (c) the person from whom discovery is sought must be the only practical source of information available to the applicants;
- (d) the person from whom discovery is sought must be reasonably compensated for his expenses arising out of compliance with the discovery order in addition to his legal costs; and
- (e) the public interests in favour of disclosure must outweigh the legitimate privacy concerns.⁴⁶⁸

This test has been described as presenting "... perhaps the ideal model of how such cases should be approached and a balance struck [between privacy and anonymity vs. access to natural justice for parties whose rights have been infringed]."⁴⁶⁹ Indeed, *BMG v Doe* was widely hailed as a victory for privacy because it preserved privacy in the face of conflict with copyright where there was insufficient evidence in support of ordering disclosure.

Although *BMG v Doe* represents the only thorough analysis and set of reasons from a Canadian court to-date in the file-sharing context, in practice Canadian courts now regularly apply the *BMG v Doe*

⁴⁶⁸ *Ibid* at paras 15, 34.

⁴⁶⁹ Lilian Edwards & Charlotte Waelde, "Online Intermediaries and Liability for Copyright Infringement" (Paper delivered at WIPO Workshop, Geneva, April 2005), online: SSRN <<http://ssrn.com/abstract=1159640>> at 54, 58. Notably, the test referred to in this report is the test developed by the lower court in *BMG v Doe* which set the threshold of the first element in the test higher than the Federal Court of Appeal set the test. The former required a plaintiff to show a 'prima facie' case whereas the latter required only a 'bona fide' case. *BMG v Doe*, *supra* note 59 at para 34. See generally Bailey, "The Substance of Procedure", *supra* note 434; Kerr & Cameron, "Nymity, P2P & ISPs", *supra* note 59.

test, and variants of this test, in ordering ISPs and other entities to identify anonymous defendants in a wide variety of cases involving pseudonymous or anonymous online activity, and in other circumstances.⁴⁷⁰ Indeed, the test enunciated in *BMG v Doe* is from one perspective not specific to the copyright context and instead represents a more general balancing of privacy interests against a

⁴⁷⁰ See generally Cameron & Michel, *supra* note 463; Alex Cameron & Nicole Melanson, "Obtaining Electronic Evidence from Non-Parties" (2010), 36 Adv Q 470. See also Berkley D Sells & Ian D Collins, "Obtaining Electronic Evidence in Special Circumstances Anton Piller Orders and Internet Defamation" in Dennis Campbell & Anita Alibekova, eds, *The Comparative Law Yearbook of International Business Volume 29* (Salzberg: Center for International Legal Studies, 2007) 196.

party's right to pursue any type of legal claim.⁴⁷¹ The type of claim advanced is not relevant, though it must be *bona fide*.⁴⁷²

Interestingly, in *Warman v Wilkins-Fournier*⁴⁷³, which is not a copyright case, the court considered the competing *Charter* interests of privacy and freedom of expression in a motion to compel a party to disclose information that may help identify other unknown defendants. The plaintiff sought an order for production from the defendant owners and operators of an online forum at <freedominion.ca>. The plaintiff sought information that would help to identify eight unnamed defendants in the action. The

⁴⁷¹ See generally Alex Cameron & Nicole Melanson, "GEA Group AG v Flex-N-Gate Corporation: Ontario Court of Appeal Emphasizes "Necessity" Requirement for Norwich Orders" (2010) 8 Commercial Litigation Review at 11 (discussing the landmark decision in *GEA Group AG v. Flex-N-Gate Corporation*, 2009 ONCA 619). C.f. Yiu, *supra* note 454 at para 65:

The BMG court's conclusion has miscast a Norwich application as primarily a battle between privacy and intellectual property, leading music publishers to declare the decision as a vindication of copyright protection. Sexton J.A.'s judgment creates the impression that privacy was ceded in this instance only because of the strong policy reasons to uphold intellectual property rights when in fact privacy must yield in every case to an injured party's quest for discovery, irrespective of the kind of right the claimant holds. A court need not explain, for example, why defamation deserves to be a tort or the policy implications of a negligence action, before granting an order for disclosure: otherwise, it would lead to the indefensible implication that one type of tort is more worthy of a Norwich remedy than another. The plaintiff's right, be it protection of intellectual property or a right against trespass is ipso facto assumed to be worthy of legal protection where there is a valid cause of action. The type of tort at issue is simply irrelevant [footnotes and citations omitted].

⁴⁷² *Ibid.* See also *Sheffield Wednesday Football Club Ltd & Ors v Hargreaves*, [2007] EWHC 2375 (QB) (rejecting identification of individuals for remarks that were "barely defamatory" at para 17).

⁴⁷³ 2009 CanLII 14054 (ON SC) [*Warman SC*]; rev'd 2010 ONSC 2126 (ON SC (Div Ct)) [*Warman Divisional Court*].

anonymous defendants had created accounts and posted messages in the online forum operated by the named defendants.

The court of first instance granted the order sought, holding that rule 30.01(1)(a) of the Ontario Rules of Civil Procedure⁴⁷⁴ “impose[d] a mandatory disclosure obligation on the parties directly” and that this obligation distinguished the case from previous cases [including *BMG v Doe*] involving motions to compel production from non-parties.⁴⁷⁵

The defendants appealed the decision and the appeal was granted. The Divisional Court held that “[i]n order to prevent the abusive use of the litigation process, disclosure cannot be automatic when *Charter* interests are engaged.”⁴⁷⁶ The court reiterated that where a party moves for productions from a non-party, the court must consider the factors set out in *BMG v Doe*.⁴⁷⁷ However in this case, where the plaintiff moved for productions from the defendants in the context of a defamation action, the court held that the motion judge should have considered the following factors:

whether the unknown alleged wrongdoer could have a reasonable expectation of anonymity in the particular circumstances;

whether the Respondent has established a prima facie case against the unknown alleged wrongdoer and is acting in good faith;

whether the Respondent has taken reasonable steps to identify the anonymous party and has been unable to do so; and

⁴⁷⁴ Rules of Civil Procedure, RRO 1990, Reg 194.

⁴⁷⁵ *Warman SC*, *supra* note 473 at paras 20-21, 30-31. See also *Morris v Johnson*, 2011 ONSC 3996.

⁴⁷⁶ *Warman Divisional Court*, *supra* note 473 at para 24.

⁴⁷⁷ *Ibid* at para 30.

whether the public interests favouring disclosure outweigh the legitimate interests of freedom of expression and right to privacy of the persons sought to be identified if the disclosure is ordered.⁴⁷⁸

The court noted that the above factors differ from those outlined in *BMG v Doe* in two key respects. First, the court need not consider the second and fourth factors set out in *BMG v Doe* as they only apply to third party respondents.⁴⁷⁹ Second, a *prima facie* standard, rather than merely a *bona fide* standard was appropriate for two reasons.

First, the concern raised in *BMG v Doe* that a *prima facie* standard would prevent the plaintiff from knowing the case it wished to assert against the defendant did not arise, because in this case the proceeding was a defamation action and thus the plaintiff knew the details of precisely what was done by each of the unknown alleged wrongdoers.⁴⁸⁰

Second, the court held, “In the circumstances of a website promoting political discussion, the possibility of a defence of fair comment reinforces the need to establish the elements of defamation on a *prima facie* basis in order to have due consideration to the interest in freedom of expression.”⁴⁸¹ The court appears to have limited the applicability of this modified test to disclosure from parties in the context of a defamation action. It remains to be seen whether this test will be adopted or modified in different contexts involving motions compelling disclosure from parties. In a subsequent ruling in the same proceeding, however, the court

⁴⁷⁸ *Ibid* at para 34.

⁴⁷⁹ *Ibid* at para 39.

⁴⁸⁰ *Ibid* at para 41.

⁴⁸¹ *Ibid* at para 42.

applied the test and granted an order compelling the website to identify anonymous defendants.⁴⁸²

Unlike technological or contractual measures and certain forms of ISP liability provisions discussed in earlier sections of this chapter, court-ordered disclosure of individuals' identity in copyright litigation puts the courts in place as a gatekeeper between copyright and privacy to ensure that disclosure is made only in appropriate cases. Courts have long played a similar role in the civil litigation and criminal law contexts.⁴⁸³ Ironically, several recent criminal law cases have adopted a particular approach to the court's role as a guardian of privacy that is openly influenced by the kinds of standard form contracting practices discussed earlier in this chapter.

*R v Ward*⁴⁸⁴, *R v Kwok*⁴⁸⁵, *R v Wilson*⁴⁸⁶ and *R v Vasic*⁴⁸⁷ address the question of whether individuals have a reasonable expectation of privacy in their name and address information held by their ISPs. In *R. v. Ward*, the court noted that the ISP's subscriber agreement permitted disclosures to law enforcement without consent, thereby negating any objectively reasonable expectation of privacy held by the target individual.⁴⁸⁸ That court held that the individual's "subjective expectation [of privacy] was not objectively reasonable having regard to all contextual factors and the totality of the circumstances", including the language of the ISP policy.⁴⁸⁹ The

⁴⁸² *Warman v Wilkins-Fournier*, 2011 ONSC 3023.

⁴⁸³ See e.g. *R v Dymont*, *supra* note 13 at para 35. See generally Cameron & Michel, *supra* note 463.

⁴⁸⁴ *R v Ward*, 2008 ONCJ 355.

⁴⁸⁵ *R v Kwok*, 2008 WL 1995837.

⁴⁸⁶ *R v Wilson* (10 February 2009), 4191/08 (Ont. S.C.J.).

⁴⁸⁷ *R v Vasic*, 2009 CanLII 6842 (ON SC)

⁴⁸⁸ *R v Ward*, *supra* note 484 at paras 68-70.

⁴⁸⁹ *Ibid* at para 68.

court in *R v Kwok* held that the individual accused in that case had a reasonable expectation of privacy that his name and address would not be disclosed by his ISP without a warrant. However, the court noted that no evidence had been led as to the terms of the ISP subscriber agreement.⁴⁹⁰ In *R. v Wilson*, the court reinforced the view that the ISP subscriber agreement dictated whether or not an individual had a reasonable expectation of privacy:

In addition, in this case the terms of the contract with the internet provider is one of the factors to be considered in assessing whether the asserted expectation of privacy is reasonable in the totality of the circumstances. That contract includes an agreement that the service provider could disclose any information necessary to satisfy any laws, regulations or other governmental request from any applicable jurisdiction. Further, the agreement contained a provision that by subscribing to the service, one consents to the collection, use and disclosure of personal information as described in the Bell Customer Privacy Policy and the Bell Code of Fair Information Practices. This privacy statement includes a provision that Bell Canada may also provide personal information to law enforcement agencies. Therefore by virtue of the contractual terms on which the internet service was provided an expectation of privacy is not reasonable.⁴⁹¹

Finally, a similar conclusion was reached in *R. v Vasic* where the court held that the terms of the subscriber agreement erased any claim that the accused had to a reasonable expectation of privacy in the information disclosed to police.⁴⁹²

⁴⁹⁰ *R v Kwok*, *supra* note 485 at 29.

⁴⁹¹ *R v Wilson*, *supra* note 486 at para 43.

⁴⁹² *R v Vasic*, *supra* note 487 at paras 54–56.

Despite being presented with an argument similar to those considered in the criminal law cases described above, the court in *BMG v. Doe* was not persuaded that the terms of the ISP subscriber agreements at issue constituted individuals' consent for the disclosure of their identities.⁴⁹³ Instead, the court held that ISPs were not entitled to disclose subscriber information without consent or a court order.⁴⁹⁴

If individuals' expectation of privacy were dependent on the terms of a contract enforced by DRM, or other standard form contracts governing access to or use of a copyright work, as *Ward*, *Kwok*, *Wilson* and *Vasic* suggest can be the case, then there are reasons to believe that individuals will in many cases be found to have little or no expectation of privacy in so far as such contracts contain the kinds of monitoring and disclosure clauses discussed earlier in this chapter. The relationship between such clauses in standard form contracts and individuals' subsequent expectation of privacy is one of the matters which will be considered in Chapter 5 as a part of how copyright ought to account for intellectual privacy.

⁴⁹³ CRIA presented the following argument to the Federal Court:

[The ISP] agreements further notify subscribers that identifying information may be disclosed if they engage in certain prohibited activities including the dissemination material that violates copyright and the use of peer-to-peer file sharing programs that causes them to exceed bandwidth limitations. Accordingly, all necessary consents have been obtained from subscribers to make the disclosures of information being requested in this motion.

CRIA Written Representations on behalf of the Plaintiffs (Applicants) for motion returnable March 12, 2004, at para 60, online: CIPPIC <http://www.cippic.ca/documents/file-sharing-lawsuits/Plaintiffs_Submissions_March_12.pdf>. However, neither the Federal Court nor the Federal Court of Appeal addressed this argument.

⁴⁹⁴ *BMG v Doe*, *supra* note 59 at para 37.

Returning to the copyright context, it is important to note the potential unintended negative consequences for privacy that the *BMG v. Doe* decision might have over the longer term:

...a number of the Court's findings in *BMG v. Doe* may quite unintentionally diminish Internet privacy in the future. ... The decision openly invites CRIA to come back to court with better evidence of wrongdoing in a future case. Such an invitation may well result in even closer scrutiny of Internet users targeted by CRIA, both to establish a reliable link between their pseudonyms and their IP address and to carefully document the kinds of activities that the individuals were engaged in for the purpose of attempting to show a *prima facie* copyright violation. It could also motivate the development of even more powerful, more invasive, surreptitious technological means of tracking people online.⁴⁹⁵

Ultimately, the test developed in *BMG v. Doe* and other similar cases is at the center of a particular space where copyright and privacy come into tension. Although there are indications that file sharing litigation may be on the decline in favour of ISP liability solutions⁴⁹⁶ and although *BMG v. Doe* test is not unique to the

⁴⁹⁵ Kerr & Cameron, "Nymity, P2P & ISPs", *supra* note 59 at 287. It must be acknowledged that the Federal Court of Appeal decision requires copyright owners to show a *bona fide* case, not a *prima facie* case. This lower threshold might lead to less invasive investigations. Of course, plaintiffs must also be mindful of the court's warning that investigations must be conducted in a way that minimizes the invasion to privacy.

⁴⁹⁶ See e.g. Sarah McBride, "Changing Tack, RIAA Ditches MediaSentry" *Wall Street Journal* (5 January 2009), online: WSJ.com <<http://online.wsj.com/article/SB123109364085551895.html>>:

In another sign of the music industry's recently announced retreat from a five-year-old antipiracy strategy, the Recording Industry Association of America has dumped the company it

copyright context, these cases and this test must form part of our analysis for how copyright might account for intellectual privacy. As suggested in this section, for example, it is important to consider how existing technology and contracting practices may affect the application of the test for disclosure of individuals' identities and to bear in mind how that test might encourage more invasive monitoring of individuals' intellectual activities. When it comes to accounting for intellectual privacy in copyright, it may be appropriate to draw a clear distinction between activities that relate to exploiting a copyright work, which typically do not involve the courts, versus copyright infringement litigation where courts are in a position to act as arbiters of competing rights and interests, including copyright and privacy. We now turn to the third and final theme through which we can gain understanding of the contemporary conflict between copyright and privacy: intermediaries.

III. Intermediaries

Situated between customers and content, it is not surprising that intermediaries such as ISPs are a focal point for many of the legal initiatives discussed in the preceding sections.⁴⁹⁷ ISPs and other intermediaries can often have a direct impact on individuals' access

used to help it gather evidence for mass lawsuits it filed against people it claimed were illegally uploading copyrighted music.

It is also notable that CRIA has not brought file sharing litigation proceedings since *BMG v Doe*, *supra* note 59. But see *Voltage Pictures LLC v Untel*, 2011 CF 1024.

⁴⁹⁷ Intermediaries are also a focal point for governments that wish to access information about individuals' online activities in connection with law enforcement, or that wish to prevent their citizens from accessing certain forms of controversial or illegal information online. See generally Jeffrey Rosen, "Google's Gatekeepers" *New York Times* (28 November 2008), online: *New York Times* <<http://www.nytimes.com/2008/11/30/magazine/30google-t.html>>.

to or use of copyright works.⁴⁹⁸ For example, ISPs can take down infringing material or terminate subscribers engaged in infringing activities. ISPs and other intermediaries in many cases are also an exclusive source of information about the identity of their customers. There are, however, a number of additional ways that ISPs and other intermediaries can be implicated in the tension between copyright and privacy.

First, ISPs and other intermediaries are potential adopters of TPM or DRM technology or similar technological measures.⁴⁹⁹ In late 2007, for example, the Motion Picture Association of America (MPAA) asked at least 25 American universities that provided internet service to their students to install special software from the MPAA on their networks.⁵⁰⁰ This software was designed to

⁴⁹⁸ See e.g. Bernt Hugenholtz & David Korteweg, "Codes of Conduct and Copyright Enforcement in Cyberspace" in IA Stamatoudi, ed, *Copyright Enforcement and the Internet, Information Law Series*, vol 21 (Alphen aan den Rijn: Kluwer Law International, 2010) at 303 (examining the impact of the rise of ISP and other service providers' codes of conduct that deal with copyright enforcement).

⁴⁹⁹ See e.g. Bill Rosenblatt, "Canadian Supreme Court Rejects ISP Music Royalties" *DRM Watch* (1 July 2004), online: *DRM Watch* <<http://www.drmwatch.com/legal/article.php/3376301>>:

[B]oth traditional ISPs and P2P file sharing networks have been studiously steering clear of any technology that has the appearance of being content-sensitive. Although this is understandable, it is somewhat unfortunate, because ISPs are natural adopters of DRM technology that would be used on behalf of their customers who are content providers.

⁵⁰⁰ Brian Krebs, "MPAA University 'Toolkit' Raises Privacy Concerns" *Washingtonpost.com* (November 2007), online: *Washingtonpost.com* <http://blog.washingtonpost.com/securityfix/2007/11/mpaa_university_toolkit_opens_1.html>. Universities have also been the subject of applications seeking disclosure of the identity of individuals alleged to have engaged in file sharing. See e.g. *London-Sire Records v Does 1-4*, *supra* note 459. See also Jacqui Cheng, "Judge says BU can't turn over infringers' IPs in P2P case" *Ars Technica* (26 November 2008), online: *Ars Technica*

pinpoint students who were engaged in file-sharing by monitoring traffic on the universities' networks.⁵⁰¹ This monitoring in and of itself raised potential privacy concerns since *all* students' traffic would be monitored in order to identify the specific students who were potentially engaged in file sharing. Additional concerns were raised when it was learned that the software 'phoned home' to MPAA and that it exposed universities' entire network traffic to access by Internet users, including "not only bandwidth usage generated by each user on the network, but also the Internet address of every Web site each user has visited."⁵⁰²

Second, intermediaries that are commercial distributors of copyright content may have interests that conflict with their subscribers to some extent. For example, cellular phone device and service providers and ISPs around the world offer music download services to their customers.⁵⁰³ In these cases, although ISPs and others can be supportive of their customers' privacy in accordance with their obligations under privacy laws⁵⁰⁴, their interests have the

<<http://arstechnica.com/news.ars/post/20081126-judge-says-bu-cant-turn-over-infringers-ips-in-p2p-case.html>>.

⁵⁰¹ Krebs, *ibid*.

⁵⁰² *Ibid*.

⁵⁰³ See Bell Canada Enterprises (BCE), Press Release, "Bell Canada Launches the Sympatico Music Store" (13 May 2004), online: BCE <<http://www.bce.ca/en/news/releases/bc/2004/05/13/71214.html>>. Another Canadian ISP, TELUS, offers music downloads in conjunction with Puretracks which can be accessed at <<http://telus.puretracks.com/>>; Eric Pfanner, "Music Industry Imitates Digital Pirates to Turn a Profit" *New York Times* (18 January 2009), online: New York Times <<http://www.nytimes.com/2009/01/19/business/worldbusiness/19digital.html>> (describing how Nokia and others are offering unlimited music downloads and build the price for the music into the price of a device or a service contract).

⁵⁰⁴ See e.g. *BMG v Doe*, *supra* note 59 at para 13; Declan McCullagh, "Verizon appeals RIAA subpoena win" *News.com* (30 January 2003), online: News.com <<http://news.com.com/2100-1023-982809.html>>; Verizon, Press Release, "RIAA v. Verizon Internet Services It's About Privacy - Not Piracy", online:

potential to conflict with their customers, including in respect of monitoring individuals' access to and use of copyright works through DRM.⁵⁰⁵ In *BMG v. Doe*, the ISP Vidéotron joined the other ISPs in refusing to disclose the identities of its customers without a court order but nevertheless "agreed with the [recording industry's] submissions on copyright infringement and adopted them as its own."⁵⁰⁶

Third, consistent with the desire of some organizations to participate in the valuable market for personal information in the digital age, some ISPs and other intermediaries have partnered with behavioural advertising companies in order to deliver targeted advertising to individuals.⁵⁰⁷ Google recently announced

<<http://newscenter.verizon.com/kit/riaa/vz.vtml>>; Matthew Broersma, "ISP sues record industry over subpoenas" *News.com* (31 July 2003), online: News.com <<http://news.com.com/2100-1027-5058107.html>>.

⁵⁰⁵ It is arguable that to some extent one of the strategies of ISPs has been to avoid being directly regulated by 'self-regulating', which in instances like this may mean partially aligning with the interests of copyright holders. I am grateful to Jane Bailey for this point. On the other hand, one of the largest online music stores in Europe, Deutsche Telekom's Musicload, has come out in opposition to DRM on the basis that DRM is burdensome from a customer service perspective. See Ken Fisher, "Musicload: 75% of customer service problems caused by DRM" *Arstechnica* (March 18, 2007), online: Arstechnica <<http://arstechnica.com/news.ars/post/20070318-75-percent-customer-problems-caused-by-drm.html>>.

⁵⁰⁶ *BMG v Doe*, *supra* note 59 at para 13.

⁵⁰⁷ See generally Chris Williams, "Brussels bounces BT-Phorm quiz back to UK.gov", *The Register* (10 October 2008), online: The Register <http://www.theregister.co.uk/2008/10/10/eu_phorm_again/>; Eric Pfanner, "3 Internet Providers in Deal for Tailored Ads" *New York Times*, (February 18, 2008), online: New York Times <<http://www.nytimes.com/2008/02/18/technology/18target.html>>; Louise Story, "A Company Promises the Deepest Data Mining Yet", *New York Times* (March 20, 2008), online: <<http://www.nytimes.com/2008/03/20/business/media/20adcoside.html>>; Harlan Yu, "Phorm's Harms Extend Beyond Privacy", *Freedom to Tinker* (April 7, 2008), online: <<http://www.freedom-to>

its intention to target advertisements to individuals using information about webpages visited and YouTube videos viewed, among other information.⁵⁰⁸ YouTube user accounts were recently modified to add “Advertising Settings”:

We want to make advertising on YouTube as useful and interesting to you as possible. To do this, we sometimes choose ads based on search terms you enter or the topic of the video you're watching. For some pages, we also choose ads that we think will reflect your interests, based on the types of videos you like to watch and other site activity. To learn more or customize your advertising preferences, please go to the Ads Preferences Manager, or to opt out of interest-based advertising completely click here.⁵⁰⁹

Targeted advertisements may also be delivered to individuals via their televisions, in some cases based on what they watch.⁵¹⁰

tinker.com/blog/harlanyu/phorms-harms-extend-beyond-privacy>; Stephanie Clifford, “Web Privacy on the Radar in Congress” *New York Times* (August 10, 2008), online: New York Times <<http://www.nytimes.com/2008/08/11/technology/11privacy.html>>. For a non-ISP example, see e.g. New York Times, “The New York Times Privacy Policy” (22 September 2008), online: New York Times <<http://www.nytimes.com/ref/membercenter/help/privacy.html>> (identifying the fact that the New York Times has partnered with no less than three companies related to online advertising, Omniture, WebTrends and Tacoda, to track usage of the NYTimes.com website and collect information about individuals’ use of the site).

⁵⁰⁸ Palmer, *supra* note 347.

⁵⁰⁹ YouTube Advertising Settings, online: <<http://www.youtube.com/account#privacy/advertising>>.

⁵¹⁰ See Stefanie Clifford, “Cable Companies Target Commercials to Audience” *New York Times* (3 March 2009), online: New York Times <<http://www.nytimes.com/2009/03/04/business/04cable.html>> (discussing cable company initiatives to deliver targeted advertisements to specific homes based on demographic information, and in one case advertisements based on how and what individuals watch using data from their remote control).

Such advertising can be based on, among other things, the Internet searches that individuals conduct, the websites that they access, and the material that they download, all of which can implicate privacy.⁵¹¹ Sir Tim Berners-Lee, seminal contributor to the invention of the world wide web, recently warned against the collection and use of individuals' Internet browsing information for such purposes, reflecting a number of the themes discussed in this dissertation:

We use the internet without a thought that a third party would know what we have just clicked on [...]

Yet the URLs [webpages] people use reveal a huge amount about their lives, loves, hates and fears. This is extremely sensitive information.

People use the web in a crisis, when wondering whether they have a sexually transmitted disease, or cancer, when wondering if they are homosexual and whether to talk about it ... to discuss political views/ [People] use the internet to inform ourselves as voters in a democracy [and] to decide what is true and what is not.

We use the internet for healthcare and social interaction.

*There will be a huge commercial pressure to release this data [...] The principle should be that it is not to be collected in the first place.*⁵¹²

⁵¹¹ Story, *supra* note 507 (reporting Phorm COO as stating that "[a]s you browse we're able to categorise all of your Internet actions"). See also Chris Williams, "BBC seen to yield over website snooping" *The Register* (6 February 2009), online: [The Register](http://www.theregister.co.uk/2009/02/06/bbc_omniture/) <http://www.theregister.co.uk/2009/02/06/bbc_omniture/>.

⁵¹² Alan Travis, "Web inventor warns against third-party internet snooping" *The Guardian* (11 March 2009), online: [The Guardian](http://www.guardian.co.uk/technology/2009/mar/11/web-inventor-warns-against-third-party-internet-snooping)

As a primary single-source of information about individuals' online activities, ISPs and other intermediaries are uniquely positioned to profit from monitoring individuals' Internet activities. Although some argue that such information is anonymous in cases where it is not linked to any identified individual⁵¹³, there are many reasons to believe that seemingly anonymous information can be capable of identifying individuals⁵¹⁴, particularly when associated with a unique identifier or an IP address and a time.⁵¹⁵ This is to say nothing of the potential that advances in technology may render individuals identifiable based on what today is not considered

<http://www.guardian.co.uk/technology/2009/mar/11/berners-lee-internet-data> [emphasis added].

⁵¹³ See Phorm, Phorm Service Privacy Policy (13 February 2008), online: Phorm <http://privacy.phorm.com/policy_services.php>:

The Phorm Service is designed to avoid collection of any Personally Identifiable Information of the user ("PII"), namely information that can be directly associated with that specific person or entity, e.g. a name, a postal address, a phone number, or an email. Phorm Service uses only Non-Personally Identifiable Information ("non-PII"), such as search terms, URLs and keywords. Phorm Service does not store or retain this information. This information is used to understand broad categories of that consumer's interests; the Phorm Service matches this with existing advertising categories ("category match"), then immediately discards this information. It is important for consumers to know that even the limited retained category match information cannot be used to identify any specific person or entity. By way of example, Phorm Service will retain only information about predefined categories of interest associated with a randomly generated ID (category matches) such as "ID #45678 is interested in IPODs."

⁵¹⁴ See e.g. Robert McMillan, "Researchers can ID anonymous Twitterers" *IT World* (26 March 2009), online: *IT World* <<http://www.itworld.com/security/65168/researchers-can-id-anonymous-twitterers>>.

⁵¹⁵ For example, since IP addresses are often capable of identifying an individual, they can be considered personal information in many cases. See generally OPC, *Leading by Example*, *supra* note 203 at § 1.1.

personal information, or the privacy implications of making decisions about everyone who falls into a particular group, notwithstanding that no particular individuals are identified.⁵¹⁶

The searches that individuals type into a search engine, for example, can reveal a great deal of information about a person and be used to identify them when combined with one another and with a unique identifier to show which searches were submitted by the same individual.⁵¹⁷ Search strings by an individual that AOL identified as “No. 4417749” led journalists to Thelma Arnold, of Lilburn, Georgia who had searched for the following, among other searches:

numb fingers

60 single men

dog that urinates on everything

landscapers in Lilburn, Ga

homes sold in shadow lake subdivision gwinnett
county georgia

⁵¹⁶ See generally Jane Bailey, “Confronting the Dragons Without and Within: Privacy’s Final Frontier? A Report on “Terra Incognita” (Paper delivered at The 29th International Conference of Data Protection and Privacy Commissioners, September 27-28, 2007), online: Privacy Horizons <http://www.privacyconference2007.gc.ca/workbooks/Terra_Incognita_summary_E.html>.

⁵¹⁷ See Declan McCullagh, “AOL’s disturbing glimpse into users’ lives” cnet (August 7, 2006), online: cnet <http://news.cnet.com/AOLs-disturbing-glimpse-into-users-lives/2100-1030_3-6103098.html>; Michael Zimmer, “The gaze of the Perfect Search Engine: Google as an *infrastructure* of dataveillance” in Amanda Spink & Michael Zimmer, eds, *Web search: Multidisciplinary perspectives* (Berlin: Springer, 2008). The Phorm service referenced in *supra*, note 507 also utilizes a unique identifier. See generally Lew McCreary, “What Was Privacy?” *Harvard Business Review* (October 2008) 123.

school supplies for Iraq children

safest place to live

the best season to visit Italy

termites

tea for good health

mature living.⁵¹⁸

On being discovered, Ms. Arnold's reaction revealed her lack of knowledge about what AOL had collected about her: "'My goodness, it's my whole personal life,' she said. 'I had no idea somebody was looking over my shoulder.' "⁵¹⁹ Other individuals would likely be equally alarmed⁵²⁰ to learn that their searches were retained or possibly made available to advertisers:

i have an interview at comcast and i need help

cheap rims for a ford focus

how can i get a job in joliet il with a theft on my background

i need to trace a cellular location

⁵¹⁸ Michael Barbaro & Tom Zeller Jr., "A Face Is Exposed for AOL Searcher No. 4417749" *New York Times* (9 August 2006), online: *New York Times* <http://www.nytimes.com/2006/08/09/technology/09aol.html?_r=1>.

⁵¹⁹ *Ibid.*

⁵²⁰ This is not to suggest that whether or not people would be alarmed should dictate whether or not a particular practice should be considered a violation intellectual privacy. As technologies and practices evolve over time, individuals' expectations (and hence whether they would be alarmed) may evolve, but that would be adopt an approach to intellectual privacy which is non-normative. To the contrary, as argued in Chapter 5, we require a normative account of intellectual privacy.

i need to know if my spouse is cheating and i need to do
a cellular trace for free

jobs with no background checks

how can i get a job with a conviction

motels in joliet il

motels in gurnee il area for under 40 dollars

how much will you pay me to donate my eggs

my boyfriend threatened me with a knife and went to
jail now im worried he'll hurt me when he gets out

my baby's father physically abuses me

how to find out if my husband is in (jail)

my husband needs free help with his anger problem in
joliet il

cash loans that you can pay back in more than 14 days

what steps do i need for an associates [sic] in paralegal
studies

back pay child support

uhaul trucking in joliet il⁵²¹

In late 2009, the popular online movie service Netflix experienced a similar problem when it released allegedly “anonymous” information on the viewing habits of 480,000 customers in

⁵²¹ Declan McCullagh, “AOL's disturbing glimpse”, *supra* note 517.

connection with a contest it was running.⁵²² However, researchers were able to quickly identify individuals by comparing information against reviews posted on the publicly available Internet Movie Database. In one case, an in-the-closet lesbian mother sued Netflix for allegedly releasing information that she believe could be used to out her.⁵²³

In December 2011, following a series of public consultations regarding behavioural advertising and related business practices, the OPC issued *Privacy and Online Behavioural Advertising Guidelines*⁵²⁴, including the following remarks regarding the use of opt-out consents:

While obtaining consent in the online environment is not without its challenges, it is possible. Opt-out consent for online behavioural advertising could be considered reasonable providing that:

- Individuals are made aware of the purposes for the practice in a manner that is clear and understandable – the purposes must be made obvious and cannot be buried in a privacy policy. Organizations should be transparent about their practices and consider how to effectively inform individuals of their online behavioural advertising practices, by using a variety of communication methods, such as online banners, layered approaches, and interactive tools;

⁵²² Dan Goodin, “Netflix cancels recommendation contest over privacy”, (12 March 2010) *The Register*, online: The Register <http://www.theregister.co.uk/2010/03/12/netflix_contest_cancelled/>.

⁵²³ Dan Goodin, “Closeted lesbian sues Netflix for privacy invasion” (21 December 2009) *The Register*, online: The Register <http://www.theregister.co.uk/2009/12/21/netflix_privacy_flap/>.

⁵²⁴ OPC, *Privacy and Online Behavioural Advertising Guidelines* (December 2011), online: OPC <http://www.priv.gc.ca/information/guide/2011/gl_ba_1112_e.pdf>.

- Individuals are informed of these purposes at or before the time of collection and provided with information about the various parties involved in online behavioural advertising;
- Individuals are able to easily opt-out of the practice—ideally at or before the time the information is collected;
- The opt-out takes effect immediately and is persistent;
- The information collected and used is limited, to the extent practicable, to non-sensitive information (avoiding sensitive information such as medical or health information); and
- Information collected and used is destroyed as soon as possible or effectively de-identified.⁵²⁵

Of course, whether they are aware of it or not, individuals searching for information online are in most cases searching for copyright works. Copyright automatically protects most original expression in Canada and other jurisdictions, with the result that most online information in the form of websites, blogs, articles, videos, audio files and electronic books is protected by copyright. In the past, individuals might have conducted similar searches for information at their local library or bookstore in conditions of relative privacy. The introduction of search engines, ISPs and other intermediaries between copyright works and individuals has brought tremendous advantages in terms of accessibility and searchability, but with an adverse impact on individuals' privacy by creating conditions of documentability on a previously-unimagined scale.

The examples above demonstrate that many intermediaries involved in the distribution of digital copyright works to

⁵²⁵ *Ibid.*

individuals can and often do monitor and collect information about individuals who access and use works. In many cases, individuals may have no expectation or understanding of such intermediaries or their information practices. These intermediaries are also constantly changing and can include websites, blogs, search engines such as Google, browser software providers such as Microsoft⁵²⁶ and Google, retailers such as Amazon, and publishers such as the New York Times. For example, Google may collect substantial information about the copyright works that individuals search for and access online, even though Google in most cases is not the copyright holder of the works at issue.

Harvard University Library, the largest academic library in the world, was an early participant in providing books from its collection to the Google Books program. The library makes clear to its patrons that their expectation of privacy is different when using Google Books to access a digital copy of the library's book, as opposed traditional forms of access provided by the library:

When anyone uses Google Book Search or other Google services, whether or not accessed via the Harvard system, Google will be collecting information about the use, which may be more extensive than the information collected by Harvard about library patrons and their use of the Harvard libraries, and Google's privacy policies will apply.⁵²⁷

⁵²⁶ John Leyden, "Fresh privacy fears over IE 8 Suggested Sites" *The Register* (2 February 2009), online: The Register <http://www.theregister.co.uk/2009/02/02/ie8_suggested_sites/> (discussing how Internet Explorer 8's 'Suggested Sites' feature collects URL history information in order to suggest websites to individuals and that "information associated with the web address, such as search terms or data you entered in forms might be included.")

⁵²⁷ Harvard University Library, "Harvard – Google Project: FAQ: Creating Access to Harvard Library Books in the Public Domain", online: Harvard <<http://hul.harvard.edu/hgproject/faq.html>>.

Indeed, under the proposed (and later rejected⁵²⁸) Google Settlement Agreement, libraries would have been required to adhere to a Security Standard, including user identification and authentication, access controls, and logging and audit requirements in connection with permitting individuals to access books in the library environment.⁵²⁹ Google's dominant position in providing access to digital books has been the subject of some controversy and concern, and was among the reasons that the proposed settlement was ultimately rejected by the court.⁵³⁰ As the Harvard University Library policy suggests would be the case, with Google as a new intermediary delivering copyright works to individual library patrons, libraries would have been forced in many cases to reconsider their role and their practices as intermediaries, particularly when licensing electronic material on behalf of their patrons.⁵³¹ Similar considerations may arise for retailers of devices that read electronic books. For example, in a desire to compete with Amazon's Kindle e-book reader which currently offers 250,000 e-book titles, Sony recently partnered with Google to make over 500,000 of Google's digitized books available on the Sony e-book

⁵²⁸ *Authors Guild v Google Inc*, *supra* note 83.

⁵²⁹ Google Settlement Agreement, *supra* note 83.

⁵³⁰ Chris Castle, "Is Google's culture grab unstoppable? Monopoly Money from Digital Books" *The Register* (31 December 2008), online: The Register <http://www.theregister.co.uk/2008/12/31/chris_castle_google_books_and_beyond/>. See also *Authors Guild v Google Inc*, *supra* note 83.

⁵³¹ For a brief but useful table comparing libraries, bookstores and Google Books, see Michael Zimmer, "Libraries vs. Bookstores vs. Google" (17 May 2007), online: michaelzimmer.org <<http://michaelzimmer.org/2007/05/17/libraries-vs-bookstores-vs-google/>>. See also International Coalition of Library Consortia (ICOLC), "Privacy Guidelines for Electronic Resources Vendors" (July 2002), online: Yale <<http://www.library.yale.edu/consortia/2002privacyguidelines.html>>.

reading device.⁵³² The practices of intermediaries between copyright works and individuals have an increasingly significant impact on individuals' intellectual privacy.

IV. Conclusions

One could be forgiven for parting from this chapter with the impression that there is an intellectual privacy conflict lurking virtually everywhere that digital copyright works are found. Nearly every interaction with a digital copyright work appears to involve monitoring or the collection of one form of personal information or another by copyright holders or the wide range of intermediaries along the copyright distribution chain. There are strong financial incentives for such entities to collect such personal information. In light of the examples discussed in this chapter, there certainly appears to be relatively little opportunity for individuals to search for, access or enjoy copyright works in the digital age under conditions of intellectual privacy. Indeed, there is relatively little opportunity for privacy in the digital age in general. The present project is one instance of a response to this much larger problem.

⁵³² See generally Brad Stone, "Sony to share in Google's e-book library" *SiliconValley.com* (18 March 2009), online: *SiliconValley.com* <http://www.siliconvalley.com/news/ci_11947049>.

CHAPTER 4:

THE NEXUS OF COPYRIGHT AND INTELLECTUAL PRIVACY

At first blush, one might conclude from Chapter 3 that copyright and intellectual privacy have come to implicate one another only over the course of the past decade since the advent of digital networked technology.⁵³³ The kinds of conflicts that have emerged in the recent past do appear to be a uniquely contemporary phenomenon. However, in light of the definition of intellectual privacy and the close links between intellectual privacy and creative endeavour discussed in Chapter 2, it should come as no great surprise that copyright and intellectual privacy also share a much older and more foundational relationship. Indeed, Sunny Handa has characterized privacy as one of the “theoretical pillars”

⁵³³ Portions of this chapter are derived in part from Alex Cameron, “Of Countrymen and Copyright: Exploring the nexus of copyright and privacy in Canada using copyright policy, data protection and the Charter” (Draft paper presented at the On the Identity Trail: Understanding the Importance and Impact of Anonymity and Authentication in a Networked Society, Paris Workshop – April 1-3, 2006, Paris, France) and Alex Cameron, “The Nexus of Intellectual Privacy and Copyright” *On the Identity Trail* (6 June 2006), online: On the Identity Trail <<http://idtrail.org/content/view/485/42/>>.

of copyright.⁵³⁴ This chapter explores the nexus of copyright and intellectual privacy.⁵³⁵

Part I of this chapter provides a basic overview of the purposes of copyright.⁵³⁶ This part does not purport to exhaustively review the jurisprudence or literature on the purposes of copyright, or to conclusively define or divine⁵³⁷ the purposes of copyright in Canada—a great deal of ink has been spilled on that subject in recent years.⁵³⁸ Instead, with reference to some of the leading legal literature on point, this part reviews how the SCC has articulated

⁵³⁴ Sunny Handa, “Understanding the Modern Law of Copyright in Canada”, (1997) McGill University (Thesis) at 160. See also Part II of this chapter.

⁵³⁵ For an examination of other potential aspects of the nexus between copyright and privacy, see e.g. Susy Frankel, “The Copyright and Privacy Nexus” (2005) 36 Victoria University of Wellington Law Review 507 (asserting that the development of a privacy tort in New Zealand and the United Kingdom has inappropriately failed to consider how copyright could inform the debate).

⁵³⁶ The purposes of Canadian copyright law have been the subject of considerable commentary and analysis, particularly in the wake of the Supreme Court of Canada decisions discussed in Part I of this chapter. See generally Scassa, “Interests in the Balance”, *supra* note 88; Carys Craig, *Copyright, Communication and Culture: Towards a Relational Theory of Copyright Law* (Cheltenham: E. Elgar, 2011) [Craig, *Copyright, Communication and Culture*]; Scassa, “Overbalancing”, *supra* note 88; Myra Tawfik, “Copyright as Droit d’auteur” (2003-2004) 17 IPJ 59; Daniel Gervais, “The Purpose of Copyright Law in Canada” (2005) UOLTJ 315 [Gervais, “The Purpose of Copyright”]; Scassa, “Overbalancing”, *supra* note 88; Abraham Drassinower, “Taking User Rights Seriously” in Geist, *In the Public Interest*, *supra* note 11 (describing “a vision of the purpose of copyright law in which the centrality of user rights is absolutely non-negotiable”) [Drassinower, “Taking User Rights Seriously”]; Carys J Craig, “Putting the Community in Communication: Dissolving the Conflict Between Freedom of Expression and Copyright” (Winter, 2006) 56 UTLJ 75 [Craig, “Putting the Community in Communication”].

⁵³⁷ Although the Supreme Court of Canada has provided welcome guidance over the past decade regarding the purposes of the *Copyright Act*, its approach of “balance” may invite more problems and questions than it answers. See generally Scassa, “Overbalancing”, *supra* note 88.

⁵³⁸ See e.g. *supra* note 536 and accompanying text.

the purposes of copyright in a series of important decisions over roughly the past decade.

Building on the above purposes of copyright and on the links between intellectual privacy, copyright and creative endeavour highlighted in Chapter 2, Part II of this chapter exposes a variety of ways that copyright already recognizes and has been shaped by intellectual privacy values. This part demonstrates that copyright already addresses intellectual privacy internally, including in the following areas: authors' right of first publication, moral rights, exceptions to copyright and levies and through related legal protections for *inter alia* library patron records and video rental records.

Finally, Part III of this chapter asserts that intellectual privacy is an essential component of copyright as a unified whole and that the purposes of copyright require the principles and rules that are proposed in Chapter 5. In other words, this part identifies some of the reasons why contemporary copyright law can and should do a better job at accounting for the value of intellectual privacy in relation to the purposes of copyright discussed herein.

I. The Purposes of Copyright

Neither the *Constitution Act, 1867*⁵³⁹ nor the *Copyright Act* contain a statement of the purpose of copyright in Canada.⁵⁴⁰ In the past,

⁵³⁹ *Constitution Act, 1867*, UK, 30 & 31 Victoria, c 3.

⁵⁴⁰ The absence of a purpose statement in the Canadian legislation is somewhat curious given that "from the very first formal copyright law, the British *Statute of Anne* (1710), the encouragement of learning and dissemination of knowledge as a means to enhance the general welfare have been chief objectives behind the grant of exclusive rights to authors": Hugenholtz & Okediji, "Conceiving an International Instrument", *supra* note 65. The full title of the *Statute of Anne* is: "An Act for the Encouragement of Learning, by vesting the Copies of Printed Books in the Authors or purchasers of such Copies, during the Times therein mentioned". In addition, the *United States*

courts interpreting the *Copyright Act* did relatively little to fill the void.⁵⁴¹ More recently, however, courts and scholars have endeavoured to articulate the purposes of copyright in Canada.⁵⁴² The SCC has shown a particular interest in copyright over roughly the past decade. As discussed below, the Court has issued a number of landmark decisions during this period which speak to a number of core copyright issues, including the very purposes of copyright in Canada.

Constitution includes an express statement of the purpose of copyright law: "To promote the Progress of Science and useful Arts, by securing for limited Times to Authors and Inventors the exclusive Right to their respective Writings and Discoveries." *United States Constitution*, art 1, § 8, cl 8. Cohen talks about the purpose of copyright in the United States as being to promote progress. However, she points out that "[c]opyright law conceives and promotes progress in two distinct but related ways: First, it seeks to increase both the quantity and quality of creative output. Second, it seeks to broaden public access to creative works." Julie Cohen, "Copyright and the Perfect Curve" (2000) 53 Vand L Rev 1799 at 1801.

⁵⁴¹ See generally Gervais, "The Purpose of Copyright", *supra* note 536 ("Copyright law should be based on an assessment of the types and levels of protection that best further its underlying policy objective(s)—assuming one can identify such objective(s). Unfortunately, until 2002, Canadian courts, practitioners and scholars had very little to rely on" at 318). The pre-2002 cases include *Compo Co v Blue Crest Music Inc.*, [1980] 1 SCR 357 at 373; *Bishop v Stevens*, [1990] 2 SCR 467, (1990), 31 CPR (3d) 394 at 477. See also *Performing Right Society, Ltd v Hammond's Bradford Brewery Co.*, [1934] 1 Ch 121 ("the *Copyright Act*, 1911 [upon which Canada's first copyright law was based]; was passed with a single object, namely, the benefit of authors of all kinds, whether the works were literary, dramatic or musical" at 127).

⁵⁴² See e.g. Craig, *Copyright, Communication and Culture*, *supra* note 536; Gervais, "The Purpose of Copyright", *supra* note 536; C J Craig, "Locke, Labour and Limiting the Author's Right: A Warning against a Lockean Approach to Copyright Law" (2002), 28 Queen's LJ 1 [Craig, "Locke, Labour and Limiting the Author's Right"]; Drassinower, "Taking User Rights Seriously", *supra* note 536; Carys J Craig, "The Evolution of Originality in Canadian Copyright Law: Authorship, Reward and the Public Interest" (2005) 2 UOLTJ 415; Robert G. Howell, "Recent Copyright Developments: Harmonization Opportunities for Canada" (2003-2004) 1 UOLTJ 149.

A. Théberge

In *Théberge v Galerie d'Art du Petit Champlain Inc*⁵⁴³, the SCC was faced with an unusual set of facts which pitted the rights of a creator, Théberge, against the property rights of Galerie d'Art du Petit Champlain, the purchaser of Théberge's works in issue. Using a chemical process, the gallery was able to literally lift ink off paper posters of Théberge's paintings. The gallery was then able to put the ink onto canvas, which it sold for considerably more than the posters would have fetched. The posters were destroyed in the process. Théberge claimed that the process *inter alia* amounted to an unauthorized reproduction of his work in violation of the *Copyright Act*.⁵⁴⁴

In concluding that there had been no reproduction of the works because no copies had been made, Binnie, J., writing for the majority, declared that:

[t]he *Copyright Act* is usually presented as a balance between promoting the public interest in the encouragement and dissemination of works of the arts and intellect and obtaining a just reward for the creator (or, more accurately, to prevent someone other than the creator from appropriating whatever benefits may be generated). [...]

The proper balance among these and other public policy objectives lies not only in recognizing the creator's rights but in giving due weight to their limited nature. In crassly economic terms it would be as inefficient to overcompensate artists and authors for the right of reproduction as it would be self-defeating to undercompensate them. Once an authorized copy of a work is sold to a member of the public, it is generally

⁵⁴³ *Théberge v Galerie d'art du Petit Champlain*, 2002 SCC 34 [Théberge].

⁵⁴⁴ Théberge also claimed that his moral rights had been violated.

for the purchaser, not the author, to determine what happens to it.

[...]

Excessive control by holders of copyrights and other forms of intellectual property may unduly limit the ability of the public domain to incorporate and embellish creative innovation in the long-term interests of society as a whole, or create practical obstacles to proper utilization.⁵⁴⁵

The above passages were widely hailed as a watershed moment in the history of copyright in Canada. The decision in *Théberge* marked the first in a series of important decisions from the SCC which placed limits on copyright owners' rights in the context of a new view of the purpose of the *Copyright Act* that requires a "balance" between authors' and users' rights.⁵⁴⁶ It is also significant that the vision of balance articulated by the Court included an express recognition of the long-term interests of society in having the ability to build on and utilize prior works. Of particular importance for the purposes of this dissertation is the Court's recognition that excessive control by copyright holders must be kept in check because it can undermine the public interest objectives of copyright.⁵⁴⁷

⁵⁴⁵ *Ibid* at paras 30-32. For further reading about how the public interest is implicated in copyright in other countries, see generally Sara Bannerman, "Copyright and the Global Good? An Examination of 'The Public Interest' in International Copyright Regimes" in Pradip Ninan Thomas & Jan Servaes, eds, *Intellectual Property Rights and Communications in Asia: Conflicting Traditions*, (New Delhi: Sage Publications, 2006).

⁵⁴⁶ In *Théberge*, the "user" owned the physical copy of the work at issue, which implicated the user's property rights to do what it pleased with its tangible property.

⁵⁴⁷ For further discussion regarding the issue of overprotectionism, see generally Handa, *supra* note 534 at 154; the dissent of Kozinski, J. of the U.S. Court of Appeals for the Ninth Circuit in *White v Samsung Elec Am, Inc*, 989 F2d 1512

These statements about the purposes of copyright represent a view of copyright as essentially utilitarian (i.e. “a means by which a broader set of public policy objectives could be achieved”⁵⁴⁸), which was a significant and important departure from past cases that had approached the *Copyright Act* principally on a proprietary view of copyright holders’ rights.⁵⁴⁹

B. CCH Canadian

In 2004, the SCC seized on another opportunity to provide direction regarding the purposes of the *Copyright Act*. In *CCH*

(9th Cir 1993) (“Nothing today, likely nothing since we tamed fire, is genuinely new: Culture, like science and technology, grows by accretion, each new creator building on the works of those who came before. Overprotection stifles the very creative forces it’s supposed to nurture” at 1513); Hugenholtz & Okediji, “Conceiving an International Instrument”, *supra* note 65 at 10. Of course, without further guidance it is extremely difficult to know how to measure when a protection or control is “excessive” or when actualization of a work is “proper” (i.e. what the optimal amount of protection is in order to fulfill the objective of balance). As Scassa points out, “the 4:3 split of the court in *Théberge* underlines the extent to which this point is contested.” Scassa, “Overbalancing”, *supra* note 88 at 187.

⁵⁴⁸ Scassa, “Overbalancing”, *supra* note 88 at 182, 188.

⁵⁴⁹ See generally, *ibid*; Gervais, “The Purpose of Copyright”, *supra* note 536. Discussing the utilitarian approach advanced in *Théberge* and continued by the Court in *SOCAN v CAIP*, *supra* note 59, Gervais notes the following at 324:

[c]opyright is not there to ‘protect’ authors (or other owners of copyright), but rather to maximize the creation, production and dissemination of knowledge and access thereto. In other words, protection is not an end but a means to achieving that purpose, which implies that the level of protection must be properly calibrated.

But see *Desputeaux v Éditions Chouette (1987) inc*, 2003 SCC 17 (“the *Copyright Act* [...] regards copyright primarily as a mechanism for protecting and transmitting the economic values associated with this type of property and with the use of it” at para 57).

*Canadian Ltd v Law Society of Upper Canada*⁵⁵⁰, a legal publisher claimed that the Law Society of Upper Canada (“LSUC”) had infringed copyright by providing a service whereby the LSUC photocopied works for researchers and allowed users of the Great Library to make copies of works using photocopiers located in the library. In each of the central issues in the case—namely, the issue of the proper standard of originality and the issue of whether the LSUC’s activities constituted “fair dealing” under the *Copyright Act*⁵⁵¹—the purpose of copyright introduced in *Théberge* played a central role in the Court’s analysis.

In a unanimous decision, the Court affirmed the purpose of copyright introduced in *Théberge*, namely “to balance the public interest in promoting the encouragement and dissemination of works of the arts and intellect and obtaining a just reward for the creator.”⁵⁵² In other words, as the Court noted in *CCH Canadian*, the *Copyright Act* has “dual objectives” (i.e. serving the public interest and providing just rewards for creators) which, along with “other public policy objectives,”⁵⁵³ must be properly balanced by the

⁵⁵⁰ *CCH Canadian Ltd. v Law Society of Upper Canada*, 2004 SCC 13 at para 63 [*CCH Canadian*].

⁵⁵¹ In addition to its findings regarding fair dealing and the purposes of copyright, the Court articulated a critical new standard for originality, concluding that an author’s work is original for the purposes of the *Copyright Act* only where it is “the product of the exercise of skill and judgment that is more than trivial.” *Ibid* at para 28. For an excellent case comment on the *CCH Canadian* decision, see Teresa Scassa, “Recalibrating Copyright Law?: A Comment on the Supreme Court of Canada’s Decision in *CCH Canadian Limited et al. v Law Society of Upper Canada*” (2004) 3 CJLT 89 [Scassa, “Recalibrating”]. See also Daniel J. Gervais, “Canadian copyright law post-CCH” (2004) 18 IPJ 131; Drassinower, “Taking User Rights Seriously”, *supra* note 536.

⁵⁵² *CCH Canadian*, *supra* note 550 at para 23.

⁵⁵³ *Théberge*, *supra* note 543 at paras 30-31. Query whether such “other public policy objectives” could and should include the protection of intellectual privacy. See Part III of this chapter.

courts when interpreting the legislation.⁵⁵⁴ In particular, the Court in *CCH Canadian* noted that fair dealing was an essential component of the balance in copyright and, in a bold step, elevated the status of fair dealing from a defence to copyright infringement to an affirmative “user right”:

⁵⁵⁴ Drassinower asserts that this “dual objective” approach distinguishes Canada from the United States, where the purpose of copyright serves only the public interest:

In the United States, the purpose of copyright law is not “dual.” On the contrary, copyright law ultimately serves the public interest and nothing other than the public interest [...]. It is trivially true, of course, that the author plays an important role in American copyright jurisprudence, but this role nowhere reaches the status of an autonomous objective in its own right: “The author’s benefit, however, is clearly a ‘secondary’ consideration. ‘The ultimate aim is, by this incentive, to stimulate artistic creativity for the general public good.’” It is also trivially true that American jurisprudence, too, casts the author-public relationship as a “balance,” but, once again, this is a balance entirely devoted to the public interest, and in which the author figures only as an instrument of the public’s interest. It is by no means a balance between author and public, in which the author’s claims (i.e. “obtaining a just reward for the creator”) arise as a matter of justice.

See Drassinower, “Taking User Rights Seriously”, *supra* note 536 at 478. See also the text accompanying *supra* note 540; Craig, “Putting the Community in Communication”, *supra* note 536 at n 108:

[in *Théberge and CCH Canadian*] the Court recognized the need for ‘copyright to protect the public’s interest in maximizing the production and dissemination of intellectual works.’ However, in light of the Court’s continued focus on authors’ right to reward, these statements fall somewhat short of endorsing a true ‘public interest’ approach.

See also Craig, “Locke, Labour and Limiting the Author’s Right”, *supra* note 542 at 18. For a slightly different take on *CCH Canadian* and the other cases discussed in this part, see Gervais, “The Purpose of Copyright”, *supra* note 536 at 317-18.

...the fair dealing exception is perhaps more properly understood as an integral part of the *Copyright Act* than simply a defence. Any act falling within the fair dealing exception will not be an infringement of copyright. The fair dealing exception, like other exceptions in the *Copyright Act*, is a user's right. In order to maintain the proper balance between the rights of a copyright owner and users' interests, it must not be interpreted restrictively. [...]

[...] the purpose of the fair dealing exception, [...] is to ensure that users are not unduly restricted in their ability to use and disseminate copyrighted works.⁵⁵⁵

The decision in *CCH Canadian* marked the second time in two years that the SCC affirmed that the purposes of copyright required that users of copyright works must not be unduly restricted (by copyright holders' rights or excessive control) in their ability to use and disseminate copyright works.

C. SOCAN v. CAIP

In *Society of Composers, Authors and Music Publishers of Canada v Canadian Assn. of Internet Providers*,⁵⁵⁶ a decision issued just a few months after *CCH Canadian*, the Court was faced with the issue of whether ISPs were liable for the transmission of copyrighted works over their networks.

In concluding that ISPs were not liable when they acted as conduits for the transmission of copyright works, the Court again reaffirmed the purposes of copyright stated in *Théberge*.⁵⁵⁷ The Court added

⁵⁵⁵ *CCH Canadian*, *supra* note 550 at paras 48, 63.

⁵⁵⁶ *SOCAN v CAIP*, *supra* note 59.

⁵⁵⁷ *Ibid* ("This Court has recently described the *Copyright Act* as providing "a balance between promoting the public interest in the encouragement and

that “[u]nder the *Copyright Act*, the rights of the copyright owner and the limitations on those rights should be read together to give ‘the fair and balanced reading that befits remedial legislation.’”⁵⁵⁸ Absent from this statement, however, is any mention of “user rights” or societal interests. Although integral to the balance to be struck in interpreting the *Copyright Act*, the absence of any mention of users in the above statement is not surprising because users were not *directly* implicated in *SOCAN v. CAIP*. Gervais endeavours to explain the issue as follows, suggesting that *SOCAN v. CAIP* should be read as implicitly accounting for user and societal interests in the balance:

In the same vein as *Théberge* and *CCH*, *SOCAN v. CAIP* sets limits to the reach of copyright and confronts it with other, potentially different policy objectives. It also shows reluctance in imposing liability on intermediaries ... [which] ... allow end-users to access human knowledge, whether in the form of books (*CCH*) or via the internet. Those end-users have a right of access and that right must not be interfered with lightly. As facilitators of this kind of access, but without control over the content that a particular user will access [...], librarians and ISPs’ interests must be safeguarded.⁵⁵⁹

The above cases, commonly known as ‘the trilogy’, marked the high-water mark of respect for user and public interest objectives in

dissemination of works of the arts and intellect and obtaining a just reward for the creator...” at para 40).

⁵⁵⁸ *Ibid* at para 88. In addition, as noted at *supra* note 127 and accompanying text, the *SOCAN v CAIP* decision contains an important statement from LeBel, J. at paras 153-155 about how copyright holders monitoring of individuals’ internet surfing and downloading activities impacts individuals’ privacy.

⁵⁵⁹ Gervais, “The Purpose of Copyright”, *supra* note 536 at 325. Gervais’ reference to “other, potentially different policy objectives” is consistent with both *Théberge* and *CCH Canadian* and may suggest one of the places that intellectual privacy could be further or better addressed in the *Copyright Act*. See also *supra* note 553 and accompanying text.

copyright in Canada. In the subsequent cases, discussed below, the SCC's stated approach to copyright arguably begins to show some cracks,⁵⁶⁰ though it is asserted here that the core appears to remain intact.

D. Robertson and Kraft

In the 2006 decision in *Robertson v Thomson Corp*⁵⁶¹, the Court was faced with a dispute between freelance authors and newspaper publishers. In a 5:4 majority, the SCC ruled for the freelance authors, finding that the reproduction of their works in electronic databases was an unauthorized reproduction of their individual articles and not a reproduction of a collective work (i.e. a newspaper). In reaching this finding, the majority did not expressly rely on the purpose of copyright as articulated in the trilogy.

On the other hand, the dissenting justices under the pen of Abella, J.⁵⁶² affirmed the Court's statements in the trilogy about the purposes of copyright. However, in what might be no more than an unsubstantive shift in semantics, Abella, J. in *Robertson* departed from the "dual objective" language used in *CCH Canadian* and instead stated the *Copyright Act* has two "purposes."⁵⁶³ In addition,

⁵⁶⁰ See Scassa, "Overbalancing", *supra* note 88 at 193. Scassa argues that the Court's "balance" approach begins to fragment even with the *SOCAN v CAIP* decision.

⁵⁶¹ *Robertson v Thomson Corp*, 2006 SCC 43 [*Robertson*].

⁵⁶² Abella J. wrote for McLachlin C.J. and Binnie, and Charron JJ., dissenting in part on the cross-appeal.

⁵⁶³ *Robertson*, *supra* note 561 ("This Court has repeatedly held that the overarching purposes of the *Copyright Act* are twofold: promoting the public interest in the encouragement and dissemination of artistic and intellectual works, and justly rewarding the creator of the work" at para 69). It is conceivable that this subtle shift in the description of the purposes of copyright may reinforce the

without explaining the basis for the comment, Abella, J. remarked that “[s]ince these purposes are often in opposition to each other, courts ‘should strive to maintain an appropriate balance between those two goals.’”⁵⁶⁴

In attempting to strike the right balance in *Robertson*, the dissenting justices reached outside of the immediate parties to the dispute (which, like *CCH Canadian* and *SOCAN v CAIP*, did not directly include users directly) and took into account the interests of those users (including authors) who it was thought would have an interest in accessing the kinds of works in issue.⁵⁶⁵ This accounting of user interests in the copyright balance, including the interests of those not before the court in the immediate case, appears similar in some respects to the approach taken in *CCH Canadian* and *SOCAN v. CAIP*.

Finally, in *Euro-Excellence v. Kraft Canada*⁵⁶⁶, Bastarache, J. (writing for LeBel and Charron JJ.) appeared to add to or modify the concept of balance articulated in the trilogy, by proposing to inject concepts of “legitimacy” and “natural limits” into his interpretation of balance.⁵⁶⁷ Although Bastarache, LeBel and Charron JJ. concurred in the result with the majority, Bastarache J.’s proposed introduction of these new concepts was squarely rejected by the majority of the justices.⁵⁶⁸ The majority agreed that the approach to

view that the balancing to be performed by the Courts in copyright cases is truly binary. See *supra* note 554 and accompanying text.

⁵⁶⁴ *Ibid* (quoting from J S McKeown, *Fox on Canadian Law of Copyright and Industrial Designs*, 4th ed (loose-leaf) at 1-13).

⁵⁶⁵ *Ibid* at para 70 (referring to the interests of “teachers, students, writers, reporters and researchers”).

⁵⁶⁶ *Euro-Excellence v Kraft Canada Inc* 2007 SCC 37 [Kraft].

⁵⁶⁷ *Ibid* at paras 78, 80, 81.

⁵⁶⁸ See e.g. *ibid* at para 3 (per Rothstein, J):

I am concerned that Bastarache J.’s approach in this case is inconsistent with this Court’s approach to statutory

interpreting the *Copyright Act* should be “purposive” but, citing *Théberge* and pre-trilogy cases which reinforced that copyright is a creature of statute, the majority concluded that the Court should interpret the statute as it is written and that the “purposive” approach did not “give judges license to substitute their policy preferences for those of Parliament.”⁵⁶⁹ Although this finding leaves intact the purposive approach to copyright developed in the trilogy, it represents a signal of how far the court is and is not prepared to take balance as a tool in interpreting the *Copyright Act*.

E. Conclusions

The framework of “balance” articulated by the SCC in the above cases is not without its potential missed opportunities⁵⁷⁰ and drawbacks⁵⁷¹ and there is some uncertainty (particularly in light of

interpretation. The “modern” or “purposive” approach requires that the words of the statute “in their grammatical and ordinary sense” be read harmoniously with the objects of the Act. It does not, however, give judges licence to substitute their policy preferences for those of Parliament. This Court has consistently held that “copyright is a creature of statute and the rights and remedies provided by the *Copyright Act* are exhaustive” [...] In my respectful view, Bastarache J.’s reasons depart from this doctrine. [citations omitted].

In addition, although they dissented in the result, Abella J and McLachlin CJ were in agreement with the majority that Bastarache J’s approach went too far. See *ibid* at para 112.

⁵⁶⁹ *Ibid* at para 3.

⁵⁷⁰ See e.g. Scassa, “Overbalancing”, *supra* note 88 at 182

[Some exceptions to copyright] enable certain uses within narrow parameters that serve a public interest [...] This public interest is most closely allied with freedom of expression values, and it is disappointing to see that in the “balance” chosen by the court, this dimension of copyright is largely ignored.

⁵⁷¹ See e.g. *ibid* where Scassa’s critique of the “balance” approach is summarized as follows at the abstract:

Kraft) about where the Court may take the concept of “balance” in future.⁵⁷² However, what has emerged from the above decisions is

The author argues that the concept of ‘balance’ in copyright law has certain limits as an interpretive tool, and offers two main critiques. First, there is a risk that the public policy dimensions of the *Copyright Act* will be oversimplified, particularly where balance is conceived as an equilibrium between two competing interests. Second, the approach suggests some sort of equality between user and creator interests that is not reflected in the statute. The author argues that the a broad-brush ‘balancing’ approach may create uncertainty and unpredictability, and, by generating a rhetoric of existing ‘balance,’ may remove the impetus for government to alter its policy direction.

⁵⁷² In some respects, the future is already here. On December 6 and 7, 2011, the Supreme Court of Canada heard the following five copyright appeals, as summarized in Giuseppina D’Agostino, “You Better Watch Out...For These Five Supreme Court Of Canada Cases” (5 December 2011), online: IP Osgoode <<http://www.iposgoode.ca/2011/12/you-better-watch-out-for-these-five-supreme-court-of-canada-cases/>>, with the decisions reserved at the time of writing:

1. *Entertainment Software Association, et al. v. Society of Composers, Authors and Music Publishers of Canada* (SCC Docket No. 33921) – Appeal of 2010 FCA 221 (A-521-07), in which the Federal Court of Appeal upheld the Copyright Board’s decision that a download of a video game that includes music is a communication of music to the public by telecommunication subject to royalties under the tariff;
2. *Province of Alberta as represented by the Minister of Education, et al. v. Canadian Copyright Licensing Agency, operating as “Access Copyright”* (SCC Docket No. 33888) – Appeal of 2010 FCA 198 (A-302-09), in which the Federal Court of Appeal upheld the Copyright Board’s certification of a tariff for the reproduction of materials for use in primary and secondary level educational institutions;
3. *Re:Sound v. Motion Picture Theatre Associations of Canada, et al.* (SCC Docket No. 34210) – Appeal of 2011 FCA 70 (A-433-09), in which the Federal Court of Appeal upheld the Copyright Board’s refusal to certify a tariff for music played in movies and on television;

a view of copyright which, seemingly more than at any time in the past, appears to recognize and strongly affirm users' rights as well as the public interest in promoting the encouragement and dissemination of works of the arts and intellect. Indeed, as Gervais observed following the trilogy:

[in *Théberge*, *CCH Canadian* and *SOCAN v. CAIP*] the Supreme Court of Canada provided Canadian copyright law with something that it had arguably been missing: a purpose. [...] Simply put, the economic purpose of copyright law is instrumentalist in nature, namely, to ensure the orderly production and distribution of, and access to, works of art and intellect. This means that a necessary degree of scarcity must be established among competing professional entities and that professional pirates must be fought and stopped. *It also means that copyright can not enter carelessly into the private sphere of individual users.*⁵⁷³

The timing of the Court's pronouncements on the purposes of copyright, and in particular the decision in *CCH Canadian*, were

4. *Rogers Communications Inc., et al. v. Society of Composers, Authors and Music Publishers of Canada* (SCC Docket No. 33922) – Appeal of 2010 FCA 220 (A-519-07 & A-520-07), in which the Federal Court of Appeal upheld the Copyright Board's decision that streaming music to computers or mobile devices is a communication to the public by telecommunication subject to the tariff; and

5. *Society of Composers, Authors and Music Publishers of Canada, et al. v. Bell Canada, et al.* (SCC Docket No. 33800) – Appeal of 2010 FCA 123 (A-514-07), in which the Federal Court of Appeal upheld the Copyright Board's decision that online, streamed previews of musical works are communications to the public by telecommunication subject to the tariff.

⁵⁷³ Gervais, "The Purpose of Copyright", *supra* note 536 at 317-18 [emphasis added]. As argued in Parts II and III of this chapter, part of the "private sphere" identified by Gervais includes conditions of intellectual privacy.

and are not only important *per se* but, notably, came at a point in time when the international and legislative copyright barometer in Canada appeared to be heading in a different direction.⁵⁷⁴ On the other hand, the approach signalled by the Court was also arguably itself *in response*⁵⁷⁵ to the kinds of conflicts between copyright and individuals' intellectual privacy identified in Chapter 3. The Court's approach also arguably brought copyright in Canada closer to its historical purposes⁵⁷⁶ and to established principles and international approaches to copyright law.⁵⁷⁷

⁵⁷⁴ See Scassa, "Recalibrating", *supra* note 551 ("[balance] may be anachronistic, insufficient, and ultimately against the grain of current legislative and international directions. The Court may well be situating itself as the last champion of a much beleaguered underdog — the ordinary user, and in this respect, the effort is welcome" at 97).

⁵⁷⁵ Gervais, "The Purpose of Copyright", *supra* note 536 at 331, 332:

It was not an obvious step for copyright on the internet to try to reach end-users who do not consider themselves as pirates nor act with intent of commercial gain. As mentioned above, I believe that this conceptual jump is precisely the point of origin of the problems we face today. And it is precisely what undergirds the Supreme Court trilogy.

⁵⁷⁶ *Ibid* at 332:

[The Trilogy] arguably aligned Canadian copyright law with its historical purpose. Even though that purpose was not stated in the statute itself, it is clear. Protection is a means to an end, and its reach, especially when it is to stop or exclude uses, should be limited where this does not serve the underlying purpose or imposes too high a social cost. *That is even more apparent where a direct conflict emerges with other rights* (e.g., *privacy*) [emphasis added].

⁵⁷⁷ Hugenholtz & Okediji, "Conceiving an International Instrument", *supra* note 65:

It is a well-established principle of copyright doctrine that the qualified grant of proprietary rights over the fruits of creative enterprise is directed first and foremost at the promotion of the public interest. [...] For over one hundred years, this public-centered rationale of copyright protection has been recognized

It remains to be seen whether and how the Court may take up “balance” and the purposes of copyright articulated above, particularly in a case where the reach of copyright or copyright holders’ practices infringes on individuals’ intellectual privacy in relation to copyright works. However, the above cases certainly give good reason to believe that the purposes of copyright in Canada will not easily tolerate or condone practices that diminish intellectual privacy in relation to copyright works. This argument is further developed below. Following a review of some of the existing links between copyright and intellectual privacy in Part II, this dissertation argues in Part III that contemporary copyright law in Canada can and should do a better job at accounting for the value of intellectual privacy in relation to the purposes of copyright discussed herein.

II. Links Between Copyright and Intellectual Privacy

This part explores a number of existing links between copyright and intellectual privacy, including a discussion of the ways that intellectual privacy has been instrumental in shaping and furthering the goals of copyright.⁵⁷⁸ The first two sections of this

and clearly articulated in all major instruments for the global regulation of copyright.

See also *Agreement on Trade-Related Aspects of Intellectual Property Rights*, April 15, 1994, *Marrakesh Agreement Establishing the World Trade Organization*, Annex 1C, 1869 UNTS 299, 33 ILM 81 (1994) [*TRIPS Agreement*] (characterizing the objective of intellectual property protection under the agreement as “the mutual advantage of producers and users of technological knowledge . . . conducive to social and economic welfare” at art 7). On the other hand, see *infra* notes 554 and 571 and accompanying text.

⁵⁷⁸ Arguably reinforcing the mutual or reciprocal nature of the relationship between copyright and privacy, Frankel asserts *inter alia* that “[i]ntellectual property, particularly copyright, ought to be a consideration in the formulation of any tort of privacy relating to information.” See Frankel, *supra* note 535 at 527. For an extremely detailed listing of “traditional rights and usages” in association with copyright works, including a wide variety of

part explore how intellectual privacy values are reflected in and consistent with certain aspects of copyright (e.g. the right of first publication, moral rights). The third section of this part discusses how copyright has also traditionally respected and protected the intellectual privacy interests of individuals, principally through the protection of users' private sphere. The fourth section of this part discusses a number of related links between copyright and privacy (though in a number of cases not intellectual privacy *per se*), including protections for library records and protection for the subjects of copyright works. Together, these sections provide support for the concepts explored in Part III.

A. Right of First Publication

The property of an author or composer of any work, whether of literature, art, or science, in such work unpublished and kept for his private use or pleasure, cannot be disputed.⁵⁷⁹

In "The Right to Privacy,"⁵⁸⁰ Warren and Brandeis sketched a picture of where copyright and privacy, including intellectual privacy, might lie in respect of one another as of 1890.⁵⁸¹ In search of the right to privacy, the eminent authors considered precedent⁵⁸²

privacy based rights and usages relating to authors, users and others, see L Chiariglione, *The Digital Media Project, Collection of TRU templates* (20 November 2004), online: Digital Media Project <<http://www.dmpf.org/open/dmp0270.zip>>.

⁵⁷⁹ *Prince Albert v Strange* (1849), 41 ER 1171 at 1178 (per Lord Cottenham LC).

⁵⁸⁰ Warren & Brandeis, *supra* note 115.

⁵⁸¹ Incidentally, a number of well-known authors were born in the same year that Warren and Brandeis published their seminal article, including Agatha Christie, Boris Pasternak, H. P. Lovecraft, Katherine Anne Porter, and Conrad Richter.

⁵⁸² See e.g. *Millar v Taylor* (1769), 4 Burr 2303 ("[i]t is certain every man has a right to keep his own sentiments, if he pleases. He has certainly a right to judge

from as early as the eighteenth century in asserting that a right to privacy was born out of *inter alia* the right of first publication in copyright but that the interest protected by the right of privacy was also independent from and broader than the scope of protection afforded by the right of first publication in copyright:

The common law secures to each individual the right of determining, ordinarily, to what extent his thoughts, sentiments, and emotions shall be communicated to others. [...] The existence of this right does not depend on the particular method of expression adopted. It is immaterial whether it be by word or by signs, in painting, by sculpture, or in music.

The right is lost only when the author himself communicates his production to the public, -- in other words, publishes it. It is entirely independent of the copyright laws, and their extension into the domain of art. The aim of those statutes is to secure to the author, composer, or artist the entire profits arising from publication; but the common-law protection enables him to control absolutely the act of publication, and in the exercise of his own discretion, to decide whether there shall be any publication at all.⁵⁸³

In examining the nature and basis of the right to control the act of first publication of a copyright work, Warren and Brandeis

whether he will make them public, or commit them only to the sight of his friends" at 2379).

⁵⁸³ Warren & Brandeis, *supra* note 115 at 198-200 [footnotes omitted]. As the quoted passage suggests, Warren and Brandeis' view of the purpose of copyright clearly influenced their view about the degree of overlap between the interests protected by copyright.

described how the right does not depend on whether the subject matter has any economic value or would otherwise be protected as intellectual property. In other words, the common law right to control the act of publication is not merely the right of control that copyright provides; nor do the interests protected by the common law right map precisely those protected by copyright. Distinguishing the right from the property based or economic principles that in their view were the purposes of copyright, Warren and Brandeis identified the right of first publication as one instance of the more general right of privacy, the now oft-quoted right “to be let alone.”⁵⁸⁴

The aspect of the relationship between copyright and intellectual privacy identified by Warren and Brandeis is based principally on the distinction between published and unpublished works. Though the right of first publication of a copyright work does not offer complete protection for intellectual privacy (because, for example, facts could be disclosed without infringing copyright), the right is a privacy-like right protected at common law and which lies at the heart of intellectual privacy.⁵⁸⁵ In fact, more than just an instance of the general right to be let alone, the first portion of the above-quoted passage shows that Warren and Brandeis identified

⁵⁸⁴ *Ibid* at 205:

These considerations lead to the conclusion that the protection afforded to thoughts, sentiments, and emotions, expressed through the medium of writing or of the arts, so far as it consists in preventing publication, is merely an instance of the enforcement of the more general right of the individual to be let alone. [...] The principle which protects personal writings and all other personal productions, not against theft and physical appropriation, but against publication in any form, is in reality not the principle of private property, but that of an inviolate personality.

⁵⁸⁵ See e.g. *Harper & Row Pubs v Nation Enterprises*, (1985) 471 US 539. See also Chapter 2, Part III.

the very form of privacy—intellectual privacy—that is the focus of this dissertation.

Given Warren and Brandeis' understanding of the purpose of copyright as being property-based or economic in nature,⁵⁸⁶ and given that the objective of their article was focussed on the search for the right to privacy, it is not surprising that they did not expressly identify or explore how the privacy interest that they had identified might be relevant to the objectives of copyright. The right of privacy in respect of copyright works was in their view "entirely independent"⁵⁸⁷ of copyright. However, we can now see that the very right about which they wrote is of course both a right to intellectual privacy and also instrumental in fulfilling the purposes of copyright. Indeed, the right of first publication has been codified in Canadian copyright law for roughly a century. Subsection 3(1) of the current *Copyright Act* provides as follows in pertinent part: [copyright], means the sole right [...], if the work is unpublished, to publish the work or any substantial part thereof [...].⁵⁸⁸ Virtually identical language was contained in the first copyright law passed in Canada.⁵⁸⁹

The right of first publication, an intellectual privacy right, helps to encourage the development and expression of new ideas.⁵⁸⁹

⁵⁸⁶ See *supra* note 583 and accompanying text.

⁵⁸⁷ Warren & Brandeis, *supra* note 115 at 200.

⁵⁸⁸ *Copyright Act, 1921*, SC 1921 c 24. ("For the purposes of this Act, 'copyright' means the sole right [...] if the work is unpublished, to publish the work or any substantial part thereof ...", s 3(1)).

⁵⁸⁹ See Chapter 2 of this dissertation. Consider also that even in the former Soviet Union, where the right of first publication was subject to an invasive state censorship regime, the right to refrain from publishing a work generally remained with authors. See generally Mira T Sundara Rajan, *Copyright and Creative Freedom: A study of post-socialist law reform* (New York: Routledge, 2006) at 142, 143. In addition, discussing a case involving the prosecution of authors for alleged anti-Soviet and anti-socialist views, Rajan notes that the court's refusal to consider unpublished drafts as representative of the author's

Echoing some of the themes discussed in Chapter 2 of this dissertation, Handa discusses the importance of intellectual privacy in the negative, noting the risk inherent in having less than absolute protection for intellectual privacy in respect of unpublished copyright works:

Making the right of privacy [protecting first publication] less than absolute, creates a chilling effect whereby confidential works will not be committed to paper for fear of their being divulged. This is similar to the approach of the courts to the U.S. first amendment law. Thus, privacy protections [protecting first publication] should be paramount. It is both an important right – considered a fundamental freedom by some – and a fragile one. Once it is lost, privacy cannot be regained. It should be removed from the reach of copyright exceptions [such as fair dealing/use or public interest exceptions].⁵⁹⁰

By avoiding the potential chilling effect described in this passage, an absolute right to intellectual privacy can be seen as encouraging the development and expression of new ideas. It creates a refuge for building ideas, an intellectual “breathing space,”⁵⁹¹ a veil behind which authors can explore ideas and develop new expressions. This right to intellectual privacy ultimately protects authors’ right to determine whether and when they will publish their expressions. It is an important creative right,⁵⁹² “the most sacred and the most legitimate, the most unassailable and the most personal of all properties.”⁵⁹³ Of course, the right of first publication in copyright

views suggests that the right of first publication is related to a right of (intellectual) privacy.

⁵⁹⁰ Handa, *supra* note 534 at 160.

⁵⁹¹ Cohen, “DRM and Privacy”, *supra* note 3 at 576-77.

⁵⁹² See e.g. Rajan, *supra* note 589 at 142-143.

⁵⁹³ Le Chapelier, 1791, quoted in Lionel Bently & Brad Sherman, *Intellectual Property Law*, 2d ed, (Cambridge: Oxford University Press, 2004) at 159.

also protects a significant potential economic benefit for authors because it ensures that they are able to reap the maximum reward from the first publication of their work.⁵⁹⁴

Though not elaborated upon, Handa proposes that one way to make intellectual privacy paramount would be to place “a statutory right of privacy in the *Copyright Act* which acknowledges the right and its absolute quality.”⁵⁹⁵ The proposal would bolster the existing right of first publication in the *Copyright Act* by ensuring that unpublished works are not subject to, for example, user rights to engage in fair dealing with such works. Quite apart from its merits, the mere fact that this proposal is made is important in terms of thinking about whether it is appropriate for copyright to protect intellectual privacy in other ways as well. There are certainly strong arguments to be made, some of which this dissertation endeavours to make, in support of the idea that copyright should appropriately account for intellectual privacy.

The importance and relevance of authors’ intellectual privacy interest in their unpublished works has also arisen in the context of orphan works.⁵⁹⁶ The U.S. Copyright Office *Report on Orphan Works* includes a discussion of this issue but in the end concludes that authors’ intellectual privacy interests should not be a bar to the inclusion of unpublished works as orphan works because it should

⁵⁹⁴ See e.g. Frankel, *supra* note 535, at 521 suggesting that:

[t]he rationale behind the right to issue to the public is to ensure that the copyright owner has the ability to seek the maximum economic reward from first publication. It is probable that the economic rationale is the main basis behind the right to issue to the public and the privacy rationale is an important, but incidental byproduct of the economics that drive copyright law.

⁵⁹⁵ Handa, *supra* note 534 at 161.

⁵⁹⁶ An orphan work is a copyright work in respect of which the copyright owner cannot be located or contacted.

be possible to get the author's consent.⁵⁹⁷ The report recommended that unpublished works be available under the orphan works provision but with a requirement that persons wishing to use orphan works be put to a higher standard in locating the author if it is determined that he or she is likely still alive, "given the privacy interests at stake."⁵⁹⁸

The right of first publication in copyright (and in some jurisdictions related rights such as the right to withdraw a work from publication once published)⁵⁹⁹ which are instances of rights of intellectual privacy, both help to (a) encourage the creation and dissemination of works of the arts and intellect and (b) obtain a just reward for the creator (because economic rewards may be greatest with the first publication of a work). In summary, there is a strong link between authors' intellectual privacy and the objectives of copyright as we now understand them in Canada.

⁵⁹⁷ United States, Register of Copyrights, "Report on Orphan Works" (January 2006), online: United States Copyright Office <<http://www.copyright.gov/orphan/orphan-report-full.pdf>> at 101:

With respect to the second interest regarding privacy, it may be the case that the author does not have any creative public reputation he seeks to protect, and thus is not naturally making himself known and locatable to prospective users. The author may have forgotten about or be unaware of the unpublished material that the user plans to publish, such as a long-lost diary or letter sent decades earlier. However, it is our view that the privacy interest is valid only during the lifetime of the author, a time during which the prospective user should be able to at least locate him.

⁵⁹⁸ *Ibid.*

⁵⁹⁹ See generally Rajan, *supra* note 589.

B. Moral Rights

A second way that intellectual privacy contributes and is connected to the objectives of copyright lies in the protection of moral rights.⁶⁰⁰ Although rights in a work are in many cases primarily rooted in copyright upon publication, that is not to say that intellectual privacy is no longer relevant. In jurisdictions with moral rights regimes, including Canada, intellectual privacy continues to play a role in furthering the goals of copyright. In Canada, authors have moral rights of integrity⁶⁰¹ of their work, and attribution (i.e. the right to be associated with the work, including the right to remain anonymous or use a pseudonym).⁶⁰²

Throughout history, authors have relied upon an ability and right to publish anonymously or pseudonymously. Well-known examples include the Brontë family⁶⁰³ and a number of authors

⁶⁰⁰ For further reading about moral rights, see e.g. David Vaver, "Authors' Moral Rights—Reform Proposals in Canada: Charter or Barter of Rights for Creators?" (1987) 25 Osgoode Hall LJ 749 [Vaver, "Authors' Moral Rights"]; Ysolde Gendreau, "Moral Rights", in Gordon F Henderson, ed, *Copyright and Confidential Information Law of Canada* (Scarborough: Carswell, 1994) at 161; Rowland Lorimer, "Intellectual Property, Moral Rights, and Trading Regimes: A Publishing Perspective" (1996) 21 Canadian Journal of Communication 267; Mike Holderness, "Moral Rights and Authors Rights: The Key to the Information Age" (1998) 1 JILT; Jonathan Herman, "Moral Rights and Canadian Copyright Reform: The Impact on Motion Picture Creators" (1990) 20 RDUS 407.

⁶⁰¹ Pursuant to section 28.2 of the *Copyright Act*, the right to integrity of a work is infringed if the work is "distorted, mutilated or otherwise modified", or "used in association with a product, service, cause, or institution," "... to the prejudice of the honour or the reputation of the author."

⁶⁰² *Copyright Act*, *supra* note 2, s 14.1. For an excellent discussion of pseudonymity, including in the copyright context, see Carole Lucock & Michael Yeo, "Naming Names: The Pseudonym in the Name of the Law" (2006) 3 UOLTJ 53.

⁶⁰³ The Brontë family drew inspiration from their neighbours and others in their community and did not want those people to know that the characters in the

participating in debates about the formation of the United States Constitution.⁶⁰⁴ Moral rights in copyright “treat the artist's oeuvre as an extension of his or her personality, possessing a dignity which is deserving of protection.”⁶⁰⁵ In Canada, section 14.1 of the *Copyright Act* provides *inter alia* that the author of a work has the right “to be associated with the work as its author by name or under a pseudonym and the right to remain anonymous.”⁶⁰⁶ Moral rights may not be assigned but may be waived in whole or in

Brontë's novels related to them. See generally Marianne Thormählen, “The Bronte pseudonyms” (1994) 75 *English Studies* 246.

⁶⁰⁴ See generally Jackson Turner Main, *The Antifederalists: Critics of the Constitution, 1781-1788* (Chapel Hill: University of North Carolina Press, 1961). See also, Carole Lucock, “Publius, the Pseudonym and Poetry” (12 September 2006), online: On the Identity Trail <http://www.anonequity.org/weblog/archives/2006/09/publius_the_pseudonym_and_poet.php>.

⁶⁰⁵ *Théberge*, *supra* note 543 at para 15. For a general discussion of authorship, see Joseph Loewenstein, *The Author's Due: Printing and the Prehistory of Copyright* (Chicago: University of Chicago Press, 2002) (tracing the emergence of possessive authorship from the establishment of the English printing industry to Statute of Anne); Craig, “Reconstructing the Author-Self”, *supra* note 102.

⁶⁰⁶ *Copyright Act*, *supra* note 2, s 14.1(1) provides that “[t]he author of a work has, subject to section 28.2, the right to the integrity of the work and, in connection with an act mentioned in section 3, the right, where reasonable in the circumstances, to be associated with the work as its author by name or under a pseudonym and the right to remain anonymous.” Notwithstanding authors' moral rights, it appears that an author may not *register* copyright in a work in Canada without providing identifying information. See e.g. Canadian Intellectual Property Office, *A Guide to Copyright* (Ottawa: Industry Canada, 2002) at 12: “[y]ou may include your pen name on your application for registration, but you must also give your full legal name. This is necessary because, without your legal name, it would be difficult to determine the full duration of the copyright, i.e. your lifetime plus 50 years”. The 2010 version of the guide states only that “[s]ince duration of a copyright is usually based on an author's lifetime, it is important to specify the author's full legal name.” See Canadian Intellectual Property Office, *A Guide to Copyrights* (Ottawa: Industry Canada 2010) at 9.

part.⁶⁰⁷ Although moral rights serve a number of different purposes and values in different contexts,⁶⁰⁸ they protect authors' "privacy and autonomy"⁶⁰⁹ and are unquestionably forms of intellectual privacy:

Copyright and privacy may be considered as protecting similar interests. Obviously, the right to privacy may be viewed as a personality right. The same goes for the moral rights granted to the author under copyright law. Thus, it could be argued that copyright and the right to privacy are branches of the same tree.⁶¹⁰

Moral rights contribute to the development and dissemination of new expression, at least to the extent that such rights encourage authors to create and disseminate works that they would not

⁶⁰⁷ *Copyright Act, ibid*, s 14.1(2). Interestingly, the proposed Google Settlement Agreement, *supra* note 83 would have addressed pseudonymous works and extended the right of pseudonymity to the rightsholder (even if not the same person as the author of the work):

...if the Book [...] was published under a pseudonym, then the Registry will only disclose that pseudonym to Google and, provided further, that if a Rightsholder requests that his, her or its identity not be disclosed to Google, then the Registry will only disclose an alias. [...] The Registry will make publicly available [...] the identity of the Registered Rightsholder, unless the Registered Rightsholder requests that such information not be made public for reasonable privacy concerns, as determined by the Registry.

⁶⁰⁸ Lucock & Yeo, *supra* note 602 ("pseudonyms are not all of a piece, and the considerations relevant to one use may be quite different for another. An important purpose of pseudonym use [...] is to mark out different identities for use in different contexts" at 105).

⁶⁰⁹ Vaver, "Authors' Moral Rights" *supra* note 600 ("[publishing under a pseudonym] protects an author's privacy and autonomy, and is an age-old and harmless device well-known to the public. It is also consistent with the law of passing off [...] at 755).

⁶¹⁰ Bygrave & Koelman, "Privacy, Data Protection and Copyright," *supra* note 61 at 37.

otherwise create or disseminate in the absence of protections for the right to remain anonymous or pseudonymous.⁶¹¹ Solove articulates the point as follows with respect to anonymity:

... anonymity in authorship is a long-standing practice that has the purpose of, among other things, promoting the unfettered expression of ideas. One form of disruption to this practice is the disclosure of concealed information. In this context, such disclosure involves revealing the identity of the author, and society protects against this disruption because of the importance of the purposes of anonymity.”⁶¹²

In summary, moral rights, and hence forms of intellectual privacy, can be viewed as instrumental in contributing to the objectives of copyright.

The foregoing sections provide some examples of ways that copyright and intellectual privacy share a complementary relationship, including in ways that further the goals of copyright policy. However, the intellectual privacy rights discussed thus far have largely been the rights of *authors*. But what of the intellectual privacy rights of individuals who access and use copyright works? Can their intellectual privacy rights possibly further the goals of copyright policy when in recent years they seem to have so often come in conflict with copyright holders as discussed in Chapter 3?

⁶¹¹ Handa argues that the inclusion of moral rights in Canada’s Act “may be viewed as consistent with a utilitarian theory of copyright law.” Handa, *supra* note 534 at 167. The Court in *Théberge* lends some support to this view while maintaining, of course, that the *Copyright Act* spells out different remedies for breach of copyright as opposed to breach of moral rights. *Théberge*, *supra* note 543 (“[t]his is not to say that moral rights do not have an economic dimension [...] or to deny that there is a moral rights aspect to copyright [...]” at para 59). For a general discussion of some of the values associated with anonymity and pseudonymity, see Kerr & Cameron, “Nymity, P2P & ISPs”, *supra* note 59.

⁶¹² Daniel J Solove, “Conceptualizing Privacy” (2002) 90 Cal L Rev 1088 at 1130.

Can intellectual privacy's utility in promoting the goals of copyright be extended to arguments in support of protecting individuals' intellectual privacy in relation to their enjoyment of copyright works?⁶¹³ The next section highlights some of the ways that *users'* intellectual privacy interests are reflected in and contribute to the objectives of copyright.

C. The Private Sphere

This part proceeds in two steps. First, this part describes how and some of the reasons why copyright has traditionally stayed out of the private sphere of individuals' access to and use of copyright works (including through limitations and exceptions to copyright such as fair dealing), and how the foregoing ensured that individuals traditionally were able to access and use works under conditions of intellectual privacy. Second, this part discusses how, when copyright first threatened to enter individuals' private sphere with technological advances in or about the 1960s, there was an express recognition of intellectual privacy values and a choice made in copyright to account for such values.

The foregoing premises lead into Part III of this chapter where it is argued that contemporary copyright law must better address intellectual privacy or else risk undermining the very values and objectives that underlie copyright and that were traditionally reflected in how copyright interacted with individual users.

1. The Traditional Position

Copyright has traditionally not interfered with individuals' freedom to access and enjoy copyright works within the private

⁶¹³ It is also important to remember that authors are also users.

sphere. Copyright has heretofore been principally concerned with protecting publishers against copying by competing publishers.⁶¹⁴

As Gervais explains, copyright law never used to concern itself with the private activities of individuals who accessed and used copyright works (i.e. activities which implicate and took place under conditions of intellectual privacy), and, importantly, it was never *meant* to do so:

The fact that copyright was not meant to be used in the private sphere is evidenced by the fact that exceptions and limitations to copyright were also written in the days of the professional intermediary as user. This explains why in several national laws, the main exceptions can be grouped into two categories: private use, which governments previously regarded as “unregulatable” and where copyright law abdicated its authority by nature; and use by specific professional intermediaries: libraries (and archives) and certain public institutions, including schools, courts and sometimes the government itself. [...] End-users always enjoyed both “room to move” because of

⁶¹⁴ See generally Gervais, “The Purpose of Copyright”, *supra* note 536; Bygrave & Koelman, “Privacy, Data Protection and Copyright”, *supra* note 61 (“Until fairly recently, neither copyright, nor copyright-holders, invaded the private sphere of users of copyrighted materials. Copyright covered only acts that constituted a commercial exploitation of a work” at 37); Natali Helberger & P Bernt Hugenholtz, “No Place Like Home for Making a Copy: Private Copying in European Copyright Law and Consumer Law” (2007) Berkeley Tech LJ 1061 [Helberger & Hugenholtz, “No Place Like Home”] at 1068-69:

Historically, private copying in Europe remained outside the scope of copyright because private copies were not considered means of communicating works to the public. The rationale of a private copying exception is informed, at least in part, by the idea of protecting the end user’s private sphere. For similar reasons, modern European copyright laws have limited the prohibition of public performance or communication to the public by exempting acts done in the private sphere.

exceptions such as fair use and rights stemming from their ownership of a physical copy.⁶¹⁵

As the above passage suggests, the term “private use” in general terms describes the uses enumerated in copyright law that individuals and others can make of copyright works, usually for personal, non-commercial purposes, without infringing copyright holders’ exclusive rights. Such uses are beyond the control of copyright holders.⁶¹⁶ Private use in Canada arises under the ‘fair dealing’ provisions⁶¹⁷ of the *Copyright Act* and in *CCH Canadian* was characterized as a positive “user right” as discussed earlier in this chapter.⁶¹⁸ Among other things, those provisions state that “[f]air dealing for the purpose of research or private study does not infringe copyright.”⁶¹⁹ Such activities are therefore within the scope of users’ rights to private use permitted by the *Copyright Act* in Canada.

Whether characterized as a user right, or as a limitation, defence or exception to a copyright holder’s rights, however, the important point for our purposes is that private use in the copyright context traditionally focuses on the types of *uses* that individuals and others can make for particular purposes without infringing

⁶¹⁵ Gervais, “The Purpose of Copyright”, *supra* note 536 at 329 [footnotes omitted]; see also Daniel Gervais, “Use of Copyright Content on the Internet: Considerations for Excludability and Collective Licensing”, in Geist, *In the Public Interest*, *supra* note 11 at 531, 548.

⁶¹⁶ See e.g. Jessica Litman, *Digital Copyright* (Amherst: Prometheus, 2006) at 18: “The presence of detailed exceptions shouldn’t obscure the fact that some uses of copyright works are not subject to copyright owners’ control at all. Copyright owners are given no control, for example, over private performance or display”; Gervais, “The Purpose of Copyright”, *supra* note 536.

⁶¹⁷ The fair dealing provisions of the *Copyright Act*, *supra* note 2 are found at s 29 – 29.2.

⁶¹⁸ See e.g. David Vaver, *Copyright Law* (Toronto: Irwin Law, 2000) at 171. See generally *CCH Canadian*, *supra* note 550.

⁶¹⁹ *Copyright Act*, *supra* note 2, s 29.

copyright, as opposed to the *conditions* under which individuals access and use copyright works in general. Although the concept of private use can certainly inform our understanding of how and why copyright ought to account for intellectual privacy, and there is no question that intellectual privacy is intimately connected with activities that constitute private use,⁶²⁰ this dissertation asserts that intellectual privacy speaks to the *conditions* under which individuals access and enjoy copyright works. In other words, while limitations and exceptions to copyright to permit private use by individual end users are key to the copyright balance, they are not necessarily sufficient to protect intellectual privacy *per se*.

In light of the preceding paragraph, it is debatable whether copyright's traditional respect for intellectual privacy came about as a matter of circumstance because of copyright's focus on professional intermediaries, or as a result of a conscious choice by policy makers.⁶²¹ Prior to the developments in mid-1960s discussed

⁶²⁰ The protection of private sphere is one of the main justifications for exceptions to copyright. See Alain Strowel, "Droit d'auteur et accès à l'information: de quelques malentendus et vrais problèmes à travers l'histoire et les développements récents" (1999) 12 CPI 185 at 198, cited in Gervais, "The Purpose of Copyright", *supra* note 536 at 329, n 47. See also P Bernt Hugenholtz, "Caching and Copyright: The Right of Temporary Copying", (2000) 22 European Intellectual Property Review 482 at 485-86:

[C]opyright protects against acts of unauthorized communication, not consumptive usage (...). [T]he mere reception or consumption of information by end-users has traditionally remained outside the scope of the copyright monopoly. Arguably, the right of privacy and the freedom of reception guaranteed in Articles 8 and 10 of the European Convention on Human Rights would be unduly restricted if the economic right encompassed mere acts of information reception or end use.

⁶²¹ See e.g. Bygrave & Koelman, "Privacy, Data Protection and Copyright", *supra* note 61 ("[private use] was generally not considered a commercial activity, and therefore not touched by copyright law. Even though the consumers' right to privacy tends not to be expressly considered in copyright law,

below, it is not clear that a conscious decision was made to protect intellectual privacy through copyright,⁶²² even though copyright's protection of the private sphere was for all intents and purposes sufficient to ensure that individuals were able to access and use copyright works under conditions of intellectual privacy and, as argued in Part III below, intellectual privacy is a necessary condition for the exercise of these user rights that are so important in the copyright balance. The rationale for private use certainly reflected individual end users' right to privacy.⁶²³ Ultimately, however, given the important value and role of intellectual privacy in relation to copyright, it matters not whether a choice had been made in the past; the choice can be made at any time. The arguments presented herein do not depend on the historical state of copyright. The historical context is merely highlighted as providing important context for the questions faced by contemporary copyright.

2. Addressing Privacy

In or about the 1960s, the proliferation of audio home taping gave rise to an important change in copyright in Germany which represented a key development in the relationship between copyright and intellectual privacy. The court decisions and legislative solutions that were later implemented resulted in the

copyright, with few exceptions, did not invade the private sphere of end-users" at 38).

⁶²² See Lessig, *Code version 2.0*, *supra* note 24 at 192:

If it's permissible to use technology to make copyrighted works available, why isn't it permissible to gather data about who uses what works? That data gathering is not part of the copyright itself; it is a byproduct of the technology. And as our tradition has never had this technical capacity before, it is hard to say a choice was made about it in the past.

⁶²³ See generally Helberger & Hugenholtz, "No Place Like Home", *supra* note 614.

creation of the German levy system which “has served as a model for all present-day levy systems.”⁶²⁴

At issue in Germany at that time was whether manufacturers of tape recording devices could be held liable for contributory copyright infringement. In the *Personalausweise*⁶²⁵ case, a milestone in the history of copyright in Germany, the German copyright collective, Gesellschaft für musikalische Aufführungs- und mechanische Vervielfältigungsrechte (GEMA), sought an order from the German Federal Supreme Court to compel device makers and distributors to collect and communicate to GEMA information about the identity of the purchasers of recording devices.

Based in part on privacy concerns,⁶²⁶ the Court denied the order sought on grounds that it would violate individual end users’ constitutionally protected private sphere:

⁶²⁴ P Bernt Hugenholtz et al, Institute for Information Law, *The Future of Levies in a Digital Environment* 9 (2003), online: IVIR <<http://www.ivir.nl/publications/other/DRM&levies-report.pdf>> [Hugenholtz, *The Future of Levies*] at 1:

Historically, copyright levy systems have been premised on the assumption that certain uses, especially private copying, of protected works cannot be controlled and exploited individually. [...] [Where] individual rights management is available [e.g. using DRM] there would appear to remain no need, and no justification, for mandatory levy systems.

⁶²⁵ BGH, 29 May 1964 - Aktz. : Ib ZR 4/63 (*Personalausweise*), in GRUR 02/1965, p. 104 [*Personalausweise*]. For excellent further reading on the *Personalausweise* case, see *ibid*.

⁶²⁶ Discussing this development, Bygrave & Koelman state that “when copyright first entered into the users’ private sphere, both the copyright-holders’ interests and the user’s right to privacy were expressly taken into consideration.” Bygrave & Koelman, “Privacy, Data Protection and Copyright”, *supra* note 61 at 37. However, it has been suggested that the Court’s decision may also have been motivated by “the *infeasibility* of licensing and enforcing copyrights within the private sphere” [emphasis added]. See Hugenholtz, *The Future of Levies*, *supra* note 624 at 38. See also (GFSC 9.6.1983)

Privacy considerations played a crucial role in the German Federal Supreme Court's landmark *Personalausweise* decision, which eventually led to the introduction of a levy on tape recording equipment in lieu of an outright prohibition on private copying. The Court considered that the monitoring of individual users' private copying behaviour would inevitably encroach upon their constitutionally protected private sphere.⁶²⁷

Following the *Personalausweise* decision, a levy was introduced on the sale of recording devices in order to compensate artists while at the same time respecting users' privacy rights.⁶²⁸ As discussed in Chapter 5, similar proposals have been discussed in response to the privacy-invasive potential of DRM and other technologies.

D. Related Protections

In addition to the major links between copyright and intellectual privacy discussed in the preceding sections, there are a number of instances where copyright and privacy (though not necessarily intellectual privacy) intersect in a more indirect or incidental way.

GRUR 1984/1: 54 (*Kopierladen*) (based on privacy rights and practical challenges, operators of copy shops should not be obliged to monitor every copy made by customers).

⁶²⁷ Helberger & Hugenholtz, "No Place Like Home", *supra* note 614 at 1069 [footnotes omitted]. See also Hugenholtz, *The Future of Levies*, *supra* note 624 ("In the opinion of the Court, although home taping constituted an infringement of copyright such measures of control would have undeniably conflicted with each individual's right to the inviolability of his home, as guaranteed by Article 13 of the *Grundgesetz*" at 11).

⁶²⁸ See generally Helberger & Hugenholtz, "No Place Like Home", *ibid*; Andrew F Christie, "Private Copying and Levy Schemes: Resolving the Paradox of Civilian and Common Law Approaches" (University of Melbourne Legal Studies Research Paper No. 116, 2004), online: SSRN <<http://ssrn.com/abstract=690521>>.

For example, there are a number of cases where copyright has been invoked to protect confidential information and in some cases what one might consider to be privacy interests.⁶²⁹ In these cases, which continue to arise, copyright has played an instrumental role in protecting intellectual privacy interests,⁶³⁰ typically in situations involving the attempted publication of personal materials such as letters.⁶³¹ In a similar way, copyright has effectively protected privacy-related interests in the area of commissioned photographs and portraits.⁶³²

In addition, as discussed in Chapter 1 of this dissertation, there are a variety of non-copyright protections for individual end users' intellectual privacy, including in respect of video rental records⁶³³ and library records.⁶³⁴ Although these are not copyright rules *per*

⁶²⁹ For a general discussion of some of the ways that copyright can provide protection for privacy interests, see Peter Jaffey, "Rights of Privacy, Confidentiality, and Publicity, and Related Rights" in Paul LC Torremans, ed, *Copyright and Human Rights: Freedom of Expression - Intellectual Property - Privacy* (The Hague: Kluwer Law International, 2004) 157.

⁶³⁰ See however *Gee v Pritchard*, [1818] 36 En Rep 670 which characterized the basis for protecting against publication of a personal letter as a property right.

⁶³¹ See e.g. *The Lady Anne Tennant v Associated Newspapers*, [1979] FSR 298 (EWHC) (copyright infringement claim by a lady in waiting to Princess Margaret against a newspaper for publishing photos taken by the lady of the Princess in private); *JD Salinger v Random House, Inc and Ian Hamilton*, 818 F2d 252 (2nd Cir 1987); *Morang & Co v Le Sueur* (1911), 45 SCR 95. These kinds of cases will undoubtedly continue to arise. Copyright has similarly been invoked by governments in attempts to restrain publication of works that contain information that for whatever reason the government wishes not to see published. See e.g. *The Commonwealth of Australia v John Fairfax & Sons Ltd.* (1980), 147 CLR 39 (HC).

⁶³² See generally Alex Cameron, "Lights, Camera,... Harmonize: Photography Issues in Copyright Reform" in Geist, *In the Public Interest*, *supra* note 11 at 408.

⁶³³ See e.g. *Video Privacy Protection Act*, *supra* note 20, which requires rental outlets to destroy rental records "as soon as practicable."

⁶³⁴ See e.g. *The Library Records Confidentiality Act*, *supra* note 10; ALA, "Interpretation of the Library Bill of Rights", *supra* note 108.

se, they address intellectual privacy protections in association with copyright works (and other information) and arguably help facilitate the public's use and dissemination of copyright works. They are thus certainly relevant to the nexus between copyright and intellectual privacy and to the objectives of copyright.

There are also cases where copyright has come into conflict with the privacy interests of *subjects* of creative works (i.e. where the privacy interest at issue does not relate to the author or end user of the work but rather to the person(s) that are depicted or described in the work). While such cases do not always implicate subjects' *intellectual* privacy interests, they are worth a brief note. One of the more recent and well-known examples of this link is the *Aubry* case discussed in Chapter 2. In that case, which was decided under the *Québec Charter* and the *Civil Code of Québec*, the Court had to grapple with how to reconcile artists' interests in creative expression in their copyright work, on the one hand, against the plaintiff's right of privacy, on the other. In no uncertain terms, the Court ruled that "[a]n artist's right to publish his or her work cannot include the right to infringe, without any justification, a fundamental right of the subject whose image appears in the work."⁶³⁵ Consistent with this approach, WIPO has provided guidance to museums in respect of the privacy interests that may arise in uses of archival film collections, particularly in respect of

⁶³⁵ *Aubry*, *supra* note 187 at paras 62, 63. The *Aubry* case was decided several years before *PIPEDA* first came into force in Canada. As an interesting aside, had the case arisen under *PIPEDA*, it is not at all certain that the result would have been the same. *PIPEDA* does not apply to "any organization in respect of personal information that the organization collects, uses or discloses for journalistic, artistic or literary purposes and does not collect, use or disclose for any other purpose." See *PIPEDA*, *supra* note 13, s 4(2)(c). Further, while copyright was not permitted to trump privacy in *Aubry*, the Federal Court of Appeal has made clear that nor will privacy trump copyright interests in cases where protecting privacy facilitates infringing activities (e.g. P2P file sharing) which arguably threaten to erode intellectual property rights: *BMG v Doe*, *supra* note 59 at paras 40, 41.

sensitive information about children who are the subject of such films.⁶³⁶

III. Contemporary Copyright Must Account for Intellectual Privacy

In the last decade, the delineation of the *conditions of access* to copyrighted works as well as the integration of viable access mechanisms into the international copyright regulatory framework have become one of the most controversial topics in international copyright law.

— Hugenholtz & Okediji⁶³⁷

⁶³⁶ Rina Elster Pantalony, *WIPO Guide on Managing Intellectual Property for Museums* (2007), online: WIPO <http://www.wipo.int/copyright/en/museums_ip/guide.html> at § 2.4.2:

...even where the copyright may have been cleared to allow for the reproduction and public performance of an audiovisual work, for example, the contents of the work, if particularly sensitive in nature and publicly performed, may violate a person's privacy rights. This is especially the case where the public performance takes place for reasons other than to report the events of the day. Works that include sensitive information about children and their personal information are particularly susceptible to claims of violations of privacy.

Although not presented as a copyright issue, the challenges inherent in managing privacy issues in respect of deceased individuals has recently arisen in the context of individuals' online accounts, including Facebook and email accounts. See e.g. Google, "Accessing a deceased person's mail" <<http://support.google.com/mail/bin/answer.py?hl=en&answer=14300>>.

⁶³⁷ Hugenholtz & Okediji, "Conceiving an International Instrument", *supra* note 65 at 7 [emphasis added], citing Daniel Gervais, *The TRIPS Agreement: Drafting History and Analysis* (Sweet & Maxwell, 1998); Ruth L. Okediji, "Back to Bilateralism? Pendulum Swings in International Intellectual Property Protection" (2003–2004) 1 UOTLJ 125.

The preceding sections of this chapter have endeavoured to describe the purposes of copyright in Canada and a number of the existing connections that exist between copyright and intellectual privacy. As described above, copyright already accounts for intellectual privacy in a number of ways and is dependent in part on different forms and conditions of intellectual privacy to achieve its objectives.

Based on the foregoing, as well as the definition of intellectual privacy in Chapter 2 and the discussion of the contemporary conflicts between copyright and intellectual privacy in Chapter 3, it is hoped that some of the reasons why intellectual privacy is essential to copyright (particularly at this point in history) are now apparent. This part endeavours to tie together a number of issues and themes discussed in this dissertation and highlights some of the important reasons why now, more than ever, copyright can and should do a better job of accounting for intellectual privacy internally.

A. Technological Developments Require a Response

The conflicts between copyright and intellectual privacy discussed in Chapter 3 have arisen largely as a result of copyright's rapid and complex penetration into the private sphere through the use of, *inter alia*, DRM technologies.⁶³⁸ Intellectual privacy interests are among the first casualties of copyright's foray into this largely new territory. Given the close relationship between copyright and particularly intellectual privacy's connection to the exceptions to

⁶³⁸ Guibault emphasizes a similar point, asserting that: "[t]he conflict between copyright protection and the users' fundamental right to privacy emerged progressively over the last century to become one of the most complex and controversial issues of contemporary copyright law." Guibault, *Copyright Limitations and Contracts*, *supra* note 395 at 47.

copyright including fair dealing,⁶³⁹ it is perhaps not surprising that privacy interests have been adversely affected by DRM technologies and other initiatives:

Entering the private sphere ... meant that copyright had to fight a new, formidable opponent: the right to privacy, [...] To summarize a complex set of arguments, it has been argued that copyright owners should not be able to control the uses of the works that are made by individual users in their private sphere, because this would amount to a violation of their privacy.⁶⁴⁰

What is surprising, however, is how very little has been done to address the issue on a legislative or policy level in Canada. While it must be acknowledged that privacy interests have made it onto the policy radar when it comes to copyright, they do not yet appear to have had great impact.⁶⁴¹ Contrasted against the positive recognition of intellectual privacy interests in the German home-taping context of the 1960s, legislators in our current digital networked society:

...seem to underestimate the users' privacy and autonomy interests. Here the copyright-holders' sphere of control manifestly overlaps the users' private sphere. Through [DRM], a copyright-holder could interfere with user privacy and autonomy to a greater extent than in the analogue environment.⁶⁴²

⁶³⁹ Guibault describes the contemporary conflict between copyright and individuals' right to privacy is "embodied in the limitation for private use". Guibault, *Copyright Limitations and Contracts*, *ibid.*

⁶⁴⁰ Gervais, "The Purpose of Copyright", *supra* note 536 at 330.

⁶⁴¹ See e.g. *supra* note 56 and accompanying text.

⁶⁴² Bygrave & Koelman, "Privacy, Data Protection and Copyright", *supra* note 61 at 37.

Further adding to the complexity of the problems that must be addressed at the nexus between copyright and intellectual privacy is the issue of contracts and consent. In the DRM context, standard terms of service and privacy policies replace and in many cases eviscerate individuals' private uses of the work and their intellectual privacy.⁶⁴³ The use of such contracts directly between copyright holders and end users is another novel development which demands attention if copyright is to adequately address intellectual privacy. For example, should we allow rights of fair dealing and intellectual privacy to be stripped away through DRM standard terms of service or a privacy policy?⁶⁴⁴ Such questions are revisited in Chapter 5.

In addition to the above, it is worth emphasizing two additional reasons why the current state of affairs is different and why copyright has not conflicted with intellectual privacy in the past. First, individuals typically did not have the means to infringe copyright works, let alone on a scale that would have an impact on the exploitation of the work – e.g. individuals could not very easily copy, distribute and sell thousands of books. Second, copyright holders have traditionally not had an efficient or effective means to invade the private sphere; there were no ways that they could track individuals' access and use of physical copies of copyright works in order to prevent or detect illegal or unauthorized activities. The

⁶⁴³ See generally Kerr, "If Left to their own Devices", *supra* note 42 at 192.

⁶⁴⁴ See *ibid* at 199:

...the legal threshold for contractual consent is not a well-suited device for protecting privacy interests. If such protections were within the exclusive domain of contract law — left up-for-grabs during the bargaining process — then there would be practically none. In too many instances, "freedom of contract" means "take-it-or-leave-it." So too, DRM licences, if left to their own devices, will offer all or nothing contracts: "either consumers agree to forgo privacy, or else they forgo access." In some instances, and privacy is certainly one of them, what people need is freedom from contract. [footnotes and citations omitted]

context in which copyright and individual privacy now interact is dramatically different.

Through exceptions like fair dealing, copyright law continues to attempt to carve out private space for individuals to access and enjoy copyright works. However, copyright holders increasingly have the legal and technological means by which to foreclose those spaces and to track individuals' private activities. This applies not only in the case of online digital content delivery services, but now also in the case of physical copies of works like CDs, as demonstrated by the infamous XCP DRM controversy discussed in Chapters 1 and 3. The scope of private, anonymous and/or autonomous use previously afforded by the ownership of tangible goods is eroding.

The modern copyright context thus requires us to consider the nature and scope of individuals' ability and potential legal right to enjoy copyright works in private, anonymously and autonomously. This chapter has argued that intellectual privacy can play a role in furthering the goals of copyright. However, copyright policy has heretofore not adequately considered the potential importance of individuals' intellectual privacy in furthering the goals of copyright. If, as the SCC has suggested, the purpose of copyright is utilitarian, aimed at balancing the economic rights of creators against promoting the public interest in the encouragement and dissemination of creative works, then we must ask what role individuals' intellectual privacy could play in that balance.

B. Copyright Objectives Support Addressing Intellectual Privacy

Copyright measures that invade privacy also act to inhibit individuals' intellectual freedoms by affecting the types of content that people choose to access or avoid. Apart from being instrumental in copyright holders' exercise of excess control, such intellectual privacy invasions themselves independently produce the same result that *Théberge* warned against. In other words, even

without the exercise of excessive control, copyright-based intellectual privacy violations have a negative impact on the purpose of copyright because they unduly inhibit the public's ability to access and enjoy creative innovation – at the very least, invading the private sphere creates a practical obstacle to proper utilization⁶⁴⁵ of copyright works. Viewed in this light, privacy invasions in connection with copyright works have the effect of undermining the purpose of copyright.

Private use is an essential part of the copyright balance in Canada—it is necessary in order for the public domain to build on creative innovation in the long-term interests of society as a whole,⁶⁴⁶ and is thus crucial to the objectives of copyright and to the fulfillment of other goals and values (which, unsurprisingly, mirror a number of the same values that are interrelated with intellectual privacy)—as Scassa asserts:

...exceptions, for research and private study, criticism or review, and for news reporting, are not simply rights to use works, they all serve the goal of ensuring that freedom of thought and expression will not be unduly chilled by an exercise of a creator's economic rights.⁶⁴⁷

Going one step further, Hugenholtz highlights some of the other values that benefit from appropriate limitations and exceptions to copyright holders' rights:

⁶⁴⁵ *Théberge*, *supra* note 543 at paras 30-31.

⁶⁴⁶ See Helberger & Hugenholtz, "No Place Like Home", *supra* note 614 at 1070:

If copyright is supposed to promote culture and serve as the "engine of free expression", the law of copyright must ... allow prospective authors to 'stand on the shoulders of giants' and freely engage in transformative uses of works of authorship. Private copying is an essential first step in this process of follow-on creation [footnotes omitted].

⁶⁴⁷ Scassa, "Overbalancing", *supra* note 88 at 190-191.

[i]t is widely recognised that the unlimited grant or exercise of rights by copyright holders without corresponding and appropriate [limitations and exceptions] has serious adverse long-term implications not only for development priorities, but indeed for the creative and innovation process itself.

Most innovation occurs incrementally by building on preceding technologies or existing knowledge, and empirical evidence in some developed countries suggests a strong correlation between the free dissemination of technological developments and know-how to growth and innovation.

Limitations and exceptions to copyrights contribute to the dissemination of knowledge, which in turn is essential for a variety of human activities and values, including liberty, the exercise of political power, and economic, social and personal advancement. [...].⁶⁴⁸

Building on this concept, it seems appropriate that the Court's recognition of user rights to private use in Canada could and should be extended to include protection or rights for users in respect of their ability to *access* works, including the *conditions* under which such access should take place, in order to not eviscerate the purposes of recognizing users' rights in the first place. There is a strong argument that intellectual privacy has always been and will continue to be a necessary condition for individuals' private use activities. Indeed, as Litman puts the point in respect of the connection between private use and intellectual privacy:

⁶⁴⁸ Bernt Hugenholtz, "Considerations for an International Instrument on Limitations and Exceptions to Copyright" (2008) 12 International Centre for Trade and Sustainable Development, online: ICTSD News and Analysis <<http://ictsd.org/i/news/bridges/11992/>>.

In addition, permitting private uses advances important copyright and noncopyright interests. Julie Cohen has written several articles exploring the idea of “intellectual privacy.” Intellectual privacy advances liberty by giving us freedom to think without surveillance and is a crucial aspect of any liberty worth having. *The ability to read works without surveillance may, for some works and some readers, be key to being able to read them at all.*⁶⁴⁹

Stated in a positive way, protecting individual privacy in relation to copyright works acts as a positive value in encouraging the creation and dissemination of copyright works. Kerr points out, for example, that “[t]he ability to disconnect one’s identity from one’s actions is of tremendous instrumental value to intellectual development and intellectual achievement.”⁶⁵⁰ This is much the same point made regarding how authors’ privacy rights help achieve the purpose of copyright, as described earlier in this chapter. Greenleaf makes the link explicit:

We expect to be able to maintain our anonymity when we pay for copyright works (at least unless there are stringent justifications to the contrary). We expect to be able to experience the use of copyright works free from surveillance, even though we pay for them. We expect that copyright owners’ control or monitoring of uses of works will be limited to specific statutory rights once we have paid for them. We extend our expectation of use in private to the fair uses for which we have not paid. All of these private uses are essential to the limits that must be placed on copyright if we are to have a creative commons, or a democratic society. Surveillance is inimical to creativity. We cannot expect people to

⁶⁴⁹ Jessica Litman, “Lawful Personal Use” (2007) 85 Tex L Rev 1871 at 1915 [footnotes omitted] [emphasis added].

⁶⁵⁰ Kerr, “If Left to their own Devices”, *supra* note 42 at 181.

“stand on the shoulders of giants” to create in the full glare of spotlights. Our traditional bundle of rights (or privileges to enjoy works in private) is no accident. It is a feature, not a bug.⁶⁵¹

Bringing these points to bear on the purpose of copyright law in Canada, it is clear that to the extent that individuals enjoy intellectual privacy in connection with their access to and enjoyment of copyright works, they are better able to develop further creative innovation, which is in the long term interests of society as a whole.⁶⁵²

A private sphere for the access and enjoyment of copyright works by individuals thus appears to be a necessary (though not a sufficient) condition for achieving the purpose of copyright. Though not usually expressed as an intellectual privacy issue, the recent trend toward increased emphasis on the importance of balance and users’ rights and the public interest in copyright is not surprising. Intellectual privacy plays an integral role in these areas, just as it plays a role in encouraging authors to create new expressions.

This recognition of the role of intellectual privacy in achieving the purposes of copyright serves to highlight the interdependence between copyright and intellectual privacy. That interdependence

⁶⁵¹ Greenleaf, “IP Phone Home”, *supra* note 48 at 19.

⁶⁵² Julie Cohen, “Information Rights and Intellectual Freedom” in Anton Vedder, ed, *Ethics and the Internet* (Antwerp: Intersentia, 2001) at 10:

A regime of information rights that assigns individuals the role of passive users of information is undesirable for both instrumental and noninstrumental reasons. Individuals play an important role in ensuring a continuing stream of new creation, and the freedom of expression is an essential component of intellectual freedom, or informational autonomy. Therefore, information law and practice must not unduly restrict the ability of individuals to become originators of information.

raises additional questions about what level of privacy protection is optimal from a copyright perspective in achieving copyright's purposes. Too little intellectual privacy will undermine copyright's purposes. However, the same might be said for too much intellectual privacy. Copyright holders will certainly argue that too much privacy in connection with copyright works in the digital environment is part of what has caused their alleged problems. In the P2P context, for example, individuals are able to copy and share copyright works under the protection of a pseudonym. While that certainly has value in encouraging the dissemination of copyright works, it might also lead to greater infringement of copyright. Although it is difficult to know where to draw the line from a copyright perspective,⁶⁵³ Chapter 5 endeavours to sketch an appropriate solution. That said, all of the foregoing strongly suggests that intellectual privacy can and must be addressed internally in copyright in order to ensure that the objectives of copyright are borne in mind in addressing intellectual privacy values in relation to copyright works.

⁶⁵³ As explored in part in Chapter 5, it has been suggested that "...the interest-balancing process will mainly consist of an assessment of what is *necessary/proportionate* for ensuring the effective enforcement of copyright-holders' legitimate interests in the light of the privacy and related interests of purchasers/users." See Bygrave & Koelman, "Privacy, Data Protection and Copyright," *supra* note 61 at 59.

CHAPTER 5:

ACCOUNTING FOR INTELLECTUAL PRIVACY WITHIN COPYRIGHT

The preceding chapters have argued in favour of accounting for intellectual privacy within copyright. In particular, building on the definition of intellectual privacy in Chapter 2 and the conflicts between copyright and intellectual privacy described in Chapter 3, it was asserted in Chapter 4 that copyright *can* (because of the nexus between copyright and intellectual privacy and the fact that intellectual privacy has been addressed in copyright in the past) and *should* (because intellectual privacy is valuable *per se*, as well as instrumental in fulfilling the objectives of copyright) do a better job of accounting for intellectual privacy in the digital age.⁶⁵⁴ The

⁶⁵⁴ In addition, it should be noted that international copyright instruments arguably permit copyright law to account for intellectual privacy as asserted in this dissertation. For example, Article 9 of the *Berne Convention for the Protection of Literary and Artistic Works*, September 9, 1886, revised at Paris July 24, 1971, 25 UST 1341, 828 UNTS 221 [*Berne Convention*] (to which Canada adheres) provides, among other things, that: "It shall be a matter for legislation in the countries of the Union to permit the reproduction of such works in certain special cases, provided that such reproduction does not conflict with a normal exploitation of the work and does not unreasonably prejudice the legitimate interests of the author." Similarly, see art 13 of the *TRIPS Agreement*, *supra* note 577. Hugenholtz and Okediji have argued that:

protection of intellectual privacy in respect of copyright works is a principle that is integral to copyright. The objective to be achieved is the attainment of a copyright system in which all are free to access and enjoy works anonymously or in private, subject only to those limited encroachments on intellectual privacy as are necessary, if any, to serve “the public interest in the encouragement and dissemination of works of the arts and intellect and obtaining a just reward for the creator.”⁶⁵⁵

With the foregoing in mind, this chapter explores what a copyright law that accounts for intellectual privacy might look like. This chapter addresses the ‘how’ of copyright and intellectual privacy – it explores potential solutions (and elements thereof) and makes five basic recommendations for rules to account for intellectual privacy within copyright. As highlighted by the preceding chapters, the rules described herein have been lacking in copyright

[t]he terms “legitimate” and “reasonable” at last inject a measure of normative meaning into the three-step test. Both terms allow an, in principle infinite, variety of public interests to be factored into the three-step equation. By the same token, these terms allow fundamental rights and freedoms, *such as the right to privacy* (which might, e.g., justify a freedom to make private copies) or freedom of expression (which could justify an entire spectrum of excepted uses), to be factored into the three-step test. [footnotes omitted] [emphasis added]

Hughenoltz & Okediji, “Conceiving an International Instrument”, *supra* note 65 at 25. See also, Daniel J. Gervais, “Towards a New Core International Copyright Norm: The Reverse Three-Step Test” (2005) 9 Marquette Intellectual Property Law 1 at 17.

⁶⁵⁵ *Théberge*, *supra* note 543 at paras 30-32. Bailey makes a similar point in respect of copyright and freedom of expression. Jane Bailey, “Deflating the Michelin Man: Protecting Users’ Rights in the Canadian Copyright Reform Process” in Geist, *In the Public Interest*, *supra* note 11, 125 at 166 [Bailey, “Deflating the Michelin Man”].

before now⁶⁵⁶ and are an essential component of contemporary copyright as a consistent and unified whole.⁶⁵⁷

This chapter proceeds in three parts. Part I explores the application of data protection law, specifically *PIPEDA*, to some of the DRM monitoring practices described in Chapter 3.⁶⁵⁸ This analysis serves dual purposes: (a) it responds to the assertion⁶⁵⁹ that data protection

⁶⁵⁶ See *supra* note 64 and accompanying text.

⁶⁵⁷ See *supra* note 4 and accompanying text.

⁶⁵⁸ Part I is derived in part from Cameron, "Learning from Data Protection Law", *supra* note 1.

⁶⁵⁹ See generally Charles Morgan, "A Canadian Policy Framework for Technological Protection Measures" (Presentation delivered at Musical Myopia, Digital Dystopia: New Media and Copyright Reform, March 23, 2007, McGill Centre for Intellectual Property Policy, Montreal), (video archive), online: McGill Centre for Intellectual Property Policy <<http://www.cipp.mcgill.ca/en/news/newsletter/89/>> ("I think it is important to acknowledge privacy concerns when you're talking about technical protection measures but in Canada we already have in place *PIPEDA* and other data protection legislation" at 173 minutes); see also Aliant Inc, et al, "A Response to the Federal Government's Consultation Paper on Digital Copyright Issues" (15 September 2001), online: Industry Canada <<http://www.ic.gc.ca/eic/site/crp-prda.nsf/fra/rp00299.html>> at paras 58-66, acknowledging that TPMs and RMI "might infringe an individual's right to privacy by tracking consumption patterns and recording on-line behaviour" and stating that:

The PIPED Act is a technology-neutral law of general application that applies to the private sector's collection, use and disclosure of personal information in the course of its commercial activities, and would naturally extend to the practices of rights owners.

The issue, therefore, is one of remedy. If a consumer of a copyright work believes that a rights holder is trying to collect personal information without his or her consent, or that the information is not necessary for the purposes of a transaction, then the consumer's recourse should be the same? In the Companies' view, it should make no difference whether the event takes place on-line or off-line, nor should it matter whether

law, not copyright law, can, will and should address the conflicts between copyright and intellectual privacy described herein and (b) it stimulates important questions and highlights elements that should be considered (and some that should be rejected) in any copyright-based solution that is aimed at addressing the nexus between copyright and intellectual privacy. Part II identifies some of the proposed models of statutory reform proffered to date in Canada that purport to address contemporary conflicts between copyright and intellectual privacy. Finally, building on the analysis in Part I and the proposals in Part II, Part III of this chapter provides five basic recommendations for rules which are designed to account for intellectual privacy within copyright in Canada.

I. Lessons from data protection law

It has been suggested that data protection legislation will address the types of conflicts between copyright and intellectual privacy described in Chapter 3, irrespective of whether Canadian law is amended in ways (e.g., protection for DRM) that may implicate intellectual privacy.⁶⁶⁰ Indeed, although the *EU Copyright Directive* recognizes that DRM monitoring can “process personal data about the consumption patterns of protected subject-matter by individuals and allow for tracing of on-line behaviour,”⁶⁶¹ it defers the privacy issue entirely to the *EU Data Protection Directive*⁶⁶²:

or not the good or service to be consumed is protected by copyright. [...]

The continued application of the [PIPEDA] will ensure that the rights of individuals regarding the collection of their personal information is applied consistently regardless of the transaction, and that a balance is maintained between the legitimate needs of rights holders to protect and manage their copyrighted works and the privacy rights of individuals.

⁶⁶⁰ See e.g. *ibid.*

⁶⁶¹ *EU Copyright Directive*, *supra* note 361 at recital 57.

⁶⁶² *EU Data Protection Directive*, *supra* note 204.

directing only that “[t]hese technical means, in their technical functions, should incorporate privacy safeguards in accordance with [the *EU Data Protection Directive*].”⁶⁶³ As argued below, such responses are unsatisfactory. There is also something perplexing about the suggestion that one law should encourage and potentially legitimize conduct which is or may be impermissible under another law.⁶⁶⁴ In other words, given the privacy invasive practices that have emerged involving the use of DRM monitoring to date (which may in many cases contravene a number of provisions of *PIPEDA*),⁶⁶⁵ it would surely be odd for copyright law to protect such technologies (and thereby encourage the diminishment of intellectual privacy),⁶⁶⁶ at least without careful consideration of the privacy-related ramifications of such protections.

In addition, while there is no doubt that *PIPEDA* will (a) apply to many of the conflicts between copyright and intellectual privacy described in Chapter 3, (b) prohibit or restrict some DRM monitoring practices, and (c) potentially inform the approach that copyright law might take to intellectual privacy, the suggestion that *PIPEDA* is a sufficient answer for such conflicts ignores the nature and significance of the relationship between copyright and intellectual privacy and does not address intellectual privacy with the goals of the copyright in mind.⁶⁶⁷ *PIPEDA* is a regulatory

⁶⁶³ *EU Copyright Directive*, *supra* note 361 at recital 57.

⁶⁶⁴ This would mean that that *PIPEDA* analysis would start from the premise that DRM technologies are legitimate, with the only issue under *PIPEDA* being whether the data protection norms have been complied with in how the particular instance of DRM at issue in a given case is deployed. I am grateful to Teresa Scassa for this point.

⁶⁶⁵ See generally CIPPIC, “Digital Rights Management and Consumer Privacy”, *supra* note 30.

⁶⁶⁶ See e.g. Yu, “Anticircumvention”, *supra* note 421 and accompanying text.

⁶⁶⁷ See generally, Bygrave & Koelman, “Privacy, Data Protection and Copyright”, *supra* note 61.

instrument of general application. As described below, *PIPEDA* is not structured in a way that permits copyright-related objectives to be adequately considered in assessing whether any particular activities that implicate intellectual privacy are or should be permissible. The analysis below reinforces the assertion in Chapter 4 that copyright objectives require that intellectual privacy be addressed within copyright – i.e. that intellectual privacy be built directly into the design of copyright rules in the digital era.⁶⁶⁸

A. Surveillance and Related Jurisprudence under *PIPEDA*

This section briefly reviews surveillance and related monitoring cases under *PIPEDA*. This body of law is relevant because, as discussed in Chapter 3, many forms of DRM use a monitoring mechanism as a component of controlling access to and use of creative works. In many cases, DRM operation is fundamentally premised on a diminishment of individuals' intellectual privacy.

As mentioned in Chapter 2,⁶⁶⁹ subsection 5(3) of *PIPEDA* contains an over-arching requirement 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.” This requirement is central in surveillance and monitoring cases under *PIPEDA*. In addition, in light of the challenges of consent as a model for the protection of intellectual privacy as described below, the appropriate purposes requirement is a potentially crucial

⁶⁶⁸ With respect to building privacy into the design of DRM technologies, as opposed to legal rules, see generally Cameron, “Infusing Privacy Norms in DRM”, *supra* note 28. More generally, the Information and Privacy Commissioner of Ontario has promoted the notion of “privacy by design” in respect of technologies and business practices which implicate privacy. See generally <www.privacybydesign.ca>.

⁶⁶⁹ See *supra* note 213 and accompanying text.

component of the effective protection of privacy in any set of rules relating to the protection of intellectual privacy.⁶⁷⁰

Section 7 of *PIPEDA* can also arise in surveillance cases and is relevant to the present analysis. 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 “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.”⁶⁷¹ Organizations often rely on this exception when using surveillance to, among other things, investigate or prevent fraud or employee misconduct.

The leading surveillance case under *PIPEDA* is *Eastmond v Canadian Pacific Railway*.⁶⁷² In this case, employees filed a complaint under *PIPEDA* 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, including parking lots, and had no ability to pan or zoom. CPR retained the

⁶⁷⁰ See generally, Lisa M Austin, “Is Consent the Foundation of Fair Information Practices? Canada’s Experience under *PIPEDA*” (2006) 56 UTLJ 181 at 215.

⁶⁷¹ Paragraph 7(1)(b) also requires that it must be “reasonable to expect that the collection with the knowledge or consent of the individual would compromise the availability or the accuracy of the information.” This requirement limits organizations’ ability to collect information without consent where the information is held by a third party (e.g. a bank or other service provide or intermediary) in circumstances where the information is unlikely to being unavailable or inaccurate if the affected individual is notified of the intended collection.

⁶⁷² *Eastmond*, *supra* note 69. The author was a member of the legal team acting for Canadian Pacific Railway in this case. 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 Canadian Privacy Law Review 121.

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 purposes of (1) deterring incidents of theft, vandalism and trespassing, (2) improving employee security, and (3) aiding in the investigation of incidents.

The OPC articulated and 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 and made the following findings, summarized after each element 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.⁶⁷³

⁶⁷³ Consistent with the first element of the *Eastmond* test, Principle 4.3.3 of *PIPEDA* states that: "[a]n organization shall not, as a condition of the supply of a product or service, require an individual to consent to the collection, use, or disclosure of information beyond that required to fulfil the explicitly specified and legitimate purposes." See also, for example, *BC PIPA*, *supra* note 211, s 7(2). The Information and Privacy Commissioner of British Columbia first interpreted this provision in *K.E. Gostlin Enterprises* [2005] BCIPCD No. 18, (Order P05-01), where it held that the word "necessary" does not mean "indispensable":

...personal information may, in some cases, be "necessary" in the sense that it is not possible to supply a product or service without the personal information or because it is legally required for the supply. But there will be cases where personal information is "necessary" even though it is not, when considered in a searching yet reasonable manner, indispensable in the sense that it is not possible to supply the product or service without the personal information.

Given the topic of this dissertation, it is an amusing coincidence that in reaching the above conclusion, the BC Commissioner relied on the Supreme

(ii) *Is camera surveillance and recording likely to be effective in meeting the specific need(s)?* 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 because the recording took place where individuals had a reduced expectation of privacy and CPR had taken a number of steps to ensure that the invasion of privacy was minimal, including:

- (A) CPR posted signs warning that cameras were present;
- (B) the cameras did not track employees because the cameras could not move;
- (C) the cameras were not targeted specifically at employees – contractors, visitors, suppliers and trespassers would all be captured by the cameras;
- (D) the cameras were not intended to aid in evaluating worker performance; and
- (E) the recordings were kept secure and the only time they were ever accessed was by CPR managers or police if an incident was reported; and

(iv) *Is there a less privacy-invasive way of achieving the same end?* CPR had considered and rejected other more

Court of Canada's interpretation of "necessary" in paragraph 2.4(1)(b) of the *Copyright Act* in the *SOCAN v CAIP* case. See *SOCAN v CAIP*, *supra* note 59 at para 91.

costly alternatives, including fences and security guards.⁶⁷⁴

Based on the foregoing findings, the court upheld CPR's installation and use of the cameras under *PIPEDA*.

The *Eastmond* four-part test has been applied in subsequent cases. Other leading surveillance cases under *PIPEDA* include a case where the OPC held that a credit card company can monitor individuals' purchasing history in order to detect fraud and for other purposes.⁶⁷⁵ Significantly for the purposes of this dissertation, a similar finding was issued in the copyright context where the OPC 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 copyright works.⁶⁷⁶ However, in reaching that finding, the OPC noted that the system was not collecting information about individuals' viewing habits.

In a case involving a subscription for satellite telecommunications services, an individual refused to provide photo identification and a credit card when the seller, in order to combat signal theft,

⁶⁷⁴ *Eastmond*, *ibid* at paras 127, 174-182. In addition, at paragraph 128 the Court noted that the four part test in fact had its origins in earlier jurisprudence:

As argued by all parties, these considerations or factors enumerated by the Privacy Commissioner are those which, over the years prior to *PIPEDA*, arbitrators adjudicating privacy issues under collective agreements involving camera surveillance have taken into account in balancing privacy interests of employees with the legitimate interests of employers.

⁶⁷⁵ OPC, "PIPEDA Case Summary #296: Language of Consent and Monitoring Activity Challenged" (20 April 2005), online: OPC <http://www.privcom.gc.ca/cf-dc/2005/296_050314_02_e.asp>.

⁶⁷⁶ OPC, "PIPEDA Case Summary #276: The Privacy Implications of Pay Per View and Piracy Prevention Measures" (27 September 2004), online: OPC <http://www.privcom.gc.ca/cf-dc/2004/cf-dc_040902_01_e.asp>.

required the individual to provide that information.⁶⁷⁷ The OPC held that the purpose of combating signal theft was a purpose that a reasonable person would consider appropriate and that the “fact of requiring a credit card—or pre-authorized payment—to purchase the equipment is necessary to fulfill the explicitly specified, and legitimate purposes, that is, contribute towards combating satellite piracy.”⁶⁷⁸ The OPC stated that “providing an ID card and credit card can reasonably contribute towards dissuading consumers from unlawfully using the equipment.”⁶⁷⁹

Finally, in a landmark 2007 case involving violations of *PIPEDA* by TJX, operator of Winners and HomeSense stores,⁶⁸⁰ the OPC 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 OPC had stated that collecting such information was inappropriate and unnecessary in this context.⁶⁸¹ In this case, however, the OPC 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

⁶⁷⁷ OPC, “*PIPEDA* Case Summary #280: A company requires two pieces of ID to purchase telecommunications equipment” (22 July 2004), online: OPC <http://www.priv.gc.ca/cf-dc/2004/cf-dc_040722_e.cfm> [*PIPEDA* Case Summary #280].

⁶⁷⁸ *Ibid.*

⁶⁷⁹ *Ibid.*

⁶⁸⁰ OPC, “Report of an Investigation into the Security, Collection and Retention of Personal Information—TJX Companies Inc./Winners Merchant International L.P.” (25 September 2007), online: OPC <http://www.privcom.gc.ca/cf-dc/2007/tjx_rep_070925_e.asp>.

⁶⁸¹ See e.g. OPC, “*PIPEDA* Case Summary #361: Retailer Requires Photo Identification to Exchange an Item” (23 February 2007), online: OPC <http://www.privcom.gc.ca/cf-dc/2006/361_20061114_e.asp>; see also, OPC, “Settled Case Summary #16: Personal Information on Receipts Removed, Return Information Limited” (13 February 2006), online: OPC <http://www.privcom.gc.ca/ser/2005/s16_051121_e.asp>.

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.

In 2008, the foregoing surveillance cases culminated in the OPC issuing *Guidelines for Overt Video Surveillance in the Private Sector*,⁶⁸² including the following ten factors for organizations to consider:

Determine whether a less privacy-invasive alternative to video surveillance would meet your needs.

Establish the business reason for conducting video surveillance and use video surveillance only for that reason.

Develop a policy on the use of video surveillance.

Limit the use and viewing range of cameras as much as possible.

Inform the public that video surveillance is taking place.

Store any recorded images in a secure location, with limited access, and destroy them when they are no longer required for business purposes.

Be ready to answer questions from the public. Individuals have the right to know who is watching them and why, what information is being captured, and what is being done with recorded images.

Give individuals access to information about themselves. This includes video images.

⁶⁸² OPC, *Guidelines for Overt Video Surveillance in the Private Sector*, (March 2008), online: OPC
<http://www.priv.gc.ca/information/guide/2008/gl_vs_080306_e.cfm>.

Educate camera operators on the obligation to protect the privacy of individuals.

Periodically evaluate the need for video surveillance.

Before considering the application of the elements of the four-part test and the above guidelines to DRM monitoring, it is important to briefly note that the question of whether a reasonable person would find DRM monitoring appropriate under subsection 5(3) of *PIPEDA* is only one of the key questions that would need to be assessed in determining whether such practices are in compliance with *PIPEDA* and other similar data protection laws. Two additional issues are discussed below: personal information and consent.

1. Personal Information

Data protection laws apply to the collection, use and disclosure of “personal information”⁶⁸³ or “personal data.”⁶⁸⁴ Thus, whether such laws, including *PIPEDA*, apply to DRM monitoring 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 contextual; for example, a name may be personal information if it is linked to other information; however, if it is not linked to other information, it may not be personal information.⁶⁸⁵ The definition of “personal information” is given a broad and expansive meaning.⁶⁸⁶ The Federal Court of Canada has adopted the

⁶⁸³ *PIPEDA*, *supra* note 13, ss 2(1) & 4(1). See also OPC, *Interpretation: Personal Information* (October 2011), online: OPC <http://www.priv.gc.ca/leg_c/interpretations_02_e.cfm>.

⁶⁸⁴ See e.g. UK Data Protection Act, *supra* note 13, s 1(1) (definition of “personal data”).

⁶⁸⁵ OPC, *PIPEDA Case Summary #205 - What is in a name?* (5 August 2003), OPC online: <http://www.privcom.gc.ca/cf-dc/2003/cf-dc_030805_03_e.asp>.

following definition of “personal information” developed by the OPC:

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.⁶⁸⁷

As described in Chapter 3, monitoring individuals’ access to and use of copyright works through DRM will in many cases involve the collection and use of personal information.⁶⁸⁸ Further, since DRM will almost always involve the collection of IP addresses as part of its operation, DRM will almost always involve the collection and use of personal information and therefore will be subject to the application of *PIPEDA*.⁶⁸⁹ For good reason,⁶⁹⁰ there are a number of

⁶⁸⁶ See e.g. *Dagg v Canada (Minister of Finance)*, [1997] 2 SCR 403 at para 68; *Canada (Information Commissioner) v Canada (Transportation Accident Investigation and Safety Board)*, 2006 FCA 157; *Canada (Information Commissioner) v Canada (Commissioner of the Royal Canadian Mounted Police)*, 2003 SCC 8 at para 23.

⁶⁸⁷ *Gordon v Canada (Health)*, 2008 FC 258 at para 34.

⁶⁸⁸ See *supra* note 149 and accompanying text. LeBel, J.’s statement in *SOCAN v CAIP* that privacy is implicated where copyright industries 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. In fact, the lack of judicial process in the disclosure of information through DRM monitoring may aggravate the potential privacy violation under *PIPEDA* since this kind of information has typically only been available to copyright owners through a judicial process.

⁶⁸⁹ For a good review and analysis of this issue, see CIPPIC, “Digital Rights Management and Consumer Privacy”, *supra* note 30.

⁶⁹⁰ See e.g. *Irwin Toy Ltd. v Doe* [2000] OJ No 3318 (SCJ) at paras 10-11:

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

findings under *PIPEDA* that hold that IP addresses can be considered personal information.⁶⁹¹ The European Union Data Protection Working Party has also concluded that IP addresses are personal data.⁶⁹²

2. Knowledge and Consent

Subject to prescribed exceptions under *PIPEDA*, “[t]he knowledge and consent of the individual are required for the collection, use, or disclosure of personal information.”⁶⁹³ In many instances of DRM

keeping with what should be perceived as being good public policy.

⁶⁹¹ See OPC, “*PIPEDA* Case Summary #25: A Broadcaster Accused of Collecting Personal Information via Web Site” (November 6, 2003), online: OPC <http://www.privcom.gc.ca/cf-dc/2001/cf-dc_011120_e.asp>; OPC, “*PIPEDA* Case Summary #315: Web-Centred Company’s Safeguards and Handling of Access Request and Privacy Complaint Questioned” (August 31, 2005), online: OPC <http://www.privcom.gc.ca/cf-dc/2005/315_20050809_03_e.asp>; OPC, “*PIPEDA* Case Summary #319: ISP’s Anti-Spam Measures Questioned” (February 13, 2006), online: OPC <http://www.privcom.gc.ca/cf-dc/2005/319_20051103_e.asp>. See also CIPPIC, “Digital Rights Management and Consumer Privacy”, *supra* note 30; Joshua J McIntyre, “Balancing Expectations of Online Privacy: Why Internet Protocol (IP) Addresses Should be Protected as Personally Identifiable Information” (2011) 60 DePaul L Rev 3.

⁶⁹² Article 29 Data Protection Working Group, “Opinion 2/2002 on the Use of Unique Identifiers in Telecommunication Terminal Equipments: The Example of IPV6” (30 May 2002), online: Europa <http://ec.europa.eu/justice_home/fsj/privacy/docs/wpdocs/2002/wp58_en.pdf>:

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.

⁶⁹³ *PIPEDA*, *supra* note 13, Principle 4.3.

operation, it will be difficult to reconcile the operation of DRM with the requirements of *PIPEDA*, including consent.⁶⁹⁴ Consent provisions are typically included in privacy policies or in licences managed by DRM. There is considerable doubt as to whether such consents should be considered adequate, as in other e-commerce contexts where individuals are required to agree to standard form licences.⁶⁹⁵ The following statement appeared in one U.S. study of 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.⁶⁹⁶

⁶⁹⁴ See e.g. *infra* note 702 and accompanying text.

⁶⁹⁵ See generally, András Jóri, "Data protection law - An Introduction" (6 April 2007) [dataprotection.eu](http://www.dataprotection.eu/pmwiki/pmwiki.php?n=Main.Privacy), online: [dataprotection.eu](http://www.dataprotection.eu/pmwiki/pmwiki.php?n=Main.Privacy) <<http://www.dataprotection.eu/pmwiki/pmwiki.php?n=Main.Privacy>> at § 3.4:

Mayer-Schönberger describes vividly the situation where the most important legal basis for the control of personal data is the individual's consent, which citizens can give due to their right to informational self-determination – this consent is usually given to the data controllers who are economically superior and in a better bargaining position, *so in reality data protection does not function as a mechanism protecting privacy. The majority "...routinely and unknowingly contracted away their right to informational self-determination as part and parcel of a business deal, in which the right itself was not even a 'bargaining chip' during negotiations.* But, since consent of the data subject had to be sufficient ground to permit information processing if one takes seriously the right to self-determination, such contractual devaluations of data protection were legally valid ..." [emphasis added] [footnotes omitted].

⁶⁹⁶ Mulligan, Han & Burstein, *supra* note 32 at 82, 83. See also Helberger et al, "INDICARE 2004", *supra* note 31 ("While unambiguously giving consent is

Others have conducted exceptional analyses on the issue of consent and concluded that there are good reasons to conclude that standard-form consents are inadequate and inappropriate in connection with DRM monitoring, both as a broader public policy matter and as a *PIPEDA* compliance matter.⁶⁹⁷ Kerr puts 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.⁶⁹⁸

Cohen articulates a similar concern, though of course the statements in the following passage beg the question of *how* we determine what levels of threats to privacy are "unacceptable" and therefore justify displacing contracts:

The single greatest obstacle to effective legal protection of privacy in intellectual consumption is not imperfect fit with the available legal theories, but the fact that each available theory gives way to contract in many, if not all, circumstances. Many believe that this deference to contract is entirely appropriate. They observe that, from the information provider's perspective, the greater

often required, data processing may be an integral part of the DRM system and as such accepted unconsciously by the consumer as part of the application. Consent is given, while it is unclear to the consumer exactly what data are processed and how" at 63).

⁶⁹⁷ See generally Kerr, "If Left to their own Devices", *supra* note 42 (considering the limits of data protection law and recommending legal countermeasures against technologies and copyright contracts that circumvent privacy law protections); see also CIPPIC, "Digital Rights Management and Consumer Privacy", *supra* note 30.

⁶⁹⁸ Kerr, *ibid* at 192.

power to withhold the transaction entirely logically includes the lesser power to impose conditions on the terms of access and use. From the individual user's perspective, these conditions may diminish privacy, but users remain free to accept or reject the terms offered to them. Privacy advocates have persuasively argued that the argument from contract is far too simplistic, and ignores both marketplace realities and important non-market considerations. Thus far, however, the law has failed to translate these challenges into a workable legal theory capable of displacing contract when threats to privacy reach unacceptable levels.⁶⁹⁹

Thus, in the foregoing ways, it is apparent that *PIPEDA*'s consent-based model may in many cases *facilitate* rather than protect against DRM monitoring practices which diminish intellectual privacy, so long as we accept that DRM licensing is a valid means of expressing consent to such practices.⁷⁰⁰ Indeed, this facilitating role is arguably in keeping with exactly what *PIPEDA* was designed to do.⁷⁰¹

⁶⁹⁹ Cohen, "DRM and Privacy", *supra* note 3 at 605.

⁷⁰⁰ A recently proposed amendment to *PIPEDA*, in the form of a new section 6.1 in the law, may in some cases help address some of the foregoing concerns regarding consent. It states: "For the purposes of clauses 4.3 to 4.3.8 of Schedule 1, the consent of an individual is only valid if it is reasonable to expect that the individual understands the nature, purpose and consequences of the collection, use or disclosure of personal information to which they are consenting." Bill C-12, *An Act to Amend the Personal Information Protection and Electronic Documents Act*, 1st Sess, 41st Parl, 2011, s 5.

⁷⁰¹ In the seminal decision in *Englander v TELUS*, *supra* note 209 at paras 38, 46, the Federal Court of Appeal made the following remarks about the purpose of *PIPEDA*:

The purpose of [*PIPEDA*] is altogether different [from the federal public sector *Privacy Act*]. It is undoubtedly directed at the protection of an individual's privacy; but it is also directed at the collection, use and disclosure of personal information by commercial organizations. It seeks to ensure that such

In addition to the consent requirements, Principle 4.4.1 of *PIPEDA* requires that “[o]rganizations shall not collect personal information indiscriminately. Both the amount and the type of information collected shall be limited to that which is necessary to fulfil the purposes identified.”⁷⁰² DRM monitoring is fundamentally at odds with this requirement: as a potentially surreptitious and continuous surveillance system, DRM tends to maximize, not limit, the collection and use of personal information.

B. Is DRM Monitoring an Appropriate Purpose?

Returning to subsection 5(3) of *PIPEDA*, quite apart from the question of whether an individual had knowledge of and gave valid consent to a particular use of DRM monitoring, there may be cases under *PIPEDA* where consent is ineffective and irrelevant because the purpose is inappropriate and thus prohibited by *PIPEDA* – i.e. the purpose cannot be consented-to.

At first glance, one might form the view that the concept of appropriate purposes may dovetail well with the vision of intellectual privacy proffered herein because, as stated by Gervais, “[t]here are valid arguments to say that one should not be able to sell one’s intellectual privacy.”⁷⁰³ Indeed, as mentioned above,⁷⁰⁴ it

collection, use and disclosure are made in a manner that reconciles, to the best possible extent, an individual’s privacy with the needs of the organization. [...]

...[E]ven though Part 1 and Schedule 1 of [*PIPEDA*] purport to protect the right of privacy, they also purport to facilitate the collection, use and disclosure of personal information by the private sector. In interpreting this legislation, the Court must strike a balance between two competing interests....

⁷⁰² *PIPEDA*, *supra* note 13, Principle 4.4.1.

⁷⁰³ Gervais, “Price of Social Norms”, *supra* note 49 at 65, quoting Cohen, “DRM and Privacy”, *supra* note 3 at 609:

has been asserted that the appropriate purposes test under subsection 5(3) of *PIPEDA* has the potential, much more so than the consent provisions in the law, to provide effective and meaningful privacy protection:

...the question of whether the information collection, use, or disclosure is appropriate within the particular transaction or relationship is dealt with under the reasonable purposes provision rather than under consent. It is reasonable purposes, therefore, that holds out the promise of requiring meaningful choices to be presented to consumers. It is reasonable purposes that have the most potential for providing a high degree of privacy protection. [...]

...[M]uch more attention needs to be paid to the interpretation of reasonable purposes so that it may fulfil its potential by providing strong privacy protection. This requires a return to the definitional difficulties that regularly surface in other regimes of privacy protection and an attempt to provide a workable understanding of privacy and its value, especially in the context of emerging technologies. To evade this responsibility through an over-emphasis on the value of individual consent is to provide inadequate and highly illusory protection for privacy.⁷⁰⁵

...intangible invasions of intellectual privacy are capable of causing great harm to individuals, and of substantially undermining shared, nonmonetizable values. Such invasions compromise rights of self-determination and undermine human dignity by eliminating the 'breathing space' for intellectual development.

⁷⁰⁴ See *supra* note 670 and accompanying text.

⁷⁰⁵ Austin, *supra* note 670 at 215. In this passage, the phrase “reasonable purposes” is used whereas this dissertation uses the phrase “appropriate purposes”.

In keeping with the above passage, this dissertation has endeavoured to articulate a deep and workable understanding of the values of intellectual privacy (particularly in respect of the nexus with the objectives of copyright). This understanding is put to the test under *PIPEDA*'s appropriate purposes test below.

1. Is monitoring necessary to meet a specific need?

The question of need under *PIPEDA* is an empirical matter weighed by the evidence submitted in support of and 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 a necessary response to those incidents.

In the case of DRM monitoring, there is conflicting evidence about whether there is a need for monitoring access to and use of copyrighted works in order to, for example, prevent, deter, or investigate copyright infringement. Proponents of DRM monitoring assert that such monitoring is needed in order to protect copyrighted works against infringement in the digital realm, often pointing to economic studies about the loss of revenues that some copyright holders claim to suffer as a result of infringement.⁷⁰⁶ This approach may well find favour under *PIPEDA*. For example, in one of the *PIPEDA* cases discussed above,⁷⁰⁷ in reaching the conclusion that requiring customers to provide identification would reasonably reduce unlawful conduct, the OPC made the following remarks regarding the need that had been demonstrated by the organization to justify the collection of information:

⁷⁰⁶ See Stan J Liebowitz, "Economists Examine File-Sharing and Music Sales" in Gilling and M Peitz, eds, *Industrial Organization and the Digital Economy*, (Cambridge: MIT Press, 2006) 145.

⁷⁰⁷ *PIPEDA* Case Summary #280, *supra* note 677.

The investigation revealed that signal theft, an unlawful activity, is a problem that affects the entire broadcasting system, as related losses in Canada are estimated at \$400 million. Like many other players in the industry, the company has undertaken specific measures to address this problem.⁷⁰⁸

Of course, copyright holders could attempt to claim a similar approach in the context of DRM monitoring.

On the other hand, opponents of DRM monitoring point to studies which indicate that copyright infringement in the digital age has not had a net-negative economic impact on certain copyright holders.⁷⁰⁹ Further evidence suggests that providing legal protection for DRM monitoring does not increase copyright holders' revenues.⁷¹⁰ Thus, on a macro level, there is some question

⁷⁰⁸ *Ibid.*

⁷⁰⁹ See Birgitte Andersen & Marion Frenz, "The Impact of Music Downloads and P2P File-Sharing on the Purchase of Music: A Study for Industry Canada" (30 October 2007), online: Industry Canada <http://strategis.ic.gc.ca/epic/site/ippd-dppi.nsf/en/h_ip01456e.html>; Felix Oberholzer-Gee & Koleman Strumpf, "The Effect of File Sharing on Record Sales An Empirical Analysis," (2007) 1 *Journal of Political Economy* 115.

⁷¹⁰ Michael Geist, "Behind the Scenes of Bill C-32: Music Copyright Collectives Say Digital Locks Won't Increase Revenue" (28 September 2011), online: MichaelGeist.ca <<http://www.michaelgeist.ca/content/view/6032/125/>>, quoting from *Submission of CMRRA-SODRAC INC. (CSI) to the Legislative Committee on Bill C-32 (January 20, 2011)*:

Contrary to the government's public statements, it is unrealistic to expect that the other measures contained in Bill C-32 as initiatives to implement the WIPO treaties would result in an increase in online music revenues for authors and publishers and musical works that will be sufficient to offset the revenue losses documented above. In fact, these measures would be unlikely to result in any substantial increase at all in legitimate online revenues for the music industry.

This can best be seen by comparing the growth in sales of legal digital downloads of music in Canada with the corresponding

as to whether there is a specific need for DRM monitoring at all. Further, given that many copyright holders do not utilize DRM monitoring, and given that some copyright holders that have utilized DRM in the past have backtracked and dropped DRM,⁷¹¹ the question of need is at best unsettled.

On a micro level, however, a specific copyright holder may be able to show that it is in a unique situation in which it can demonstrate a specific need for DRM monitoring. Using the *Eastmond* case as an example, assume for the sake of argument that non-CPR rail yards in Canada did not have any security problems and in fact were 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.

As demonstrated by the foregoing, the first element of the *Eastmond* test appears to be extremely challenging to apply in the context of DRM monitoring. This is not surprising. Debate regarding contemporary copyright is highly charged and extremely divisive. Given the myriad economic and policy choices at play in the copyright sphere, where experts, policy makers, stakeholders and

growth pattern in the United States, where the WIPO treaties were implemented in 1998. Apple's iTunes Music Store launched in Canada in December 2004, 18 months later than in the U.S. Since then, the rate of growth of online sales in Canada has every year been much more rapid than in the United States. Nielsen SoundScan data show that, between 2005 and 2010 the sale of paid, legal downloads of individual songs or single tracks increased by 914% in Canada, compared to 232% in the U.S. Digital album sales increased 1207% in Canada, compared to 431% in the U.S.

As a result, CSI fundamentally disagrees with the suggestion that the "modernization" measures in Bill C-32 are in any way necessary in order to improve the fortunes of the music industry.

⁷¹¹ See *supra* note 422 and accompanying text.

legislators often do not agree on the approach that should be taken in copyright, we can hardly expect the OPC (with her limited resources and privacy-focused mandate) to single-handedly resolve the complex interplay and conflicts that have emerged between copyright and intellectual privacy. Nor is it appropriate that she do so. Indeed, as the history of copyright and technological advances have repeatedly demonstrated, copyright holders' perceived "needs" at a particular point in time can be misleading or misplaced; for example:

[in the Sony betamax case] [m]otion picture producers argued that if individuals could videotape copyrighted motion pictures off-the-air for their own personal use, the industry would be ruined. The Court disagreed, and today, some sixteen years after the dire predictions, a very large portion of the movie industry's income is from the sale and rental of videocassettes of motion pictures.⁷¹²

The foregoing highlights the dangers inherent in basing DRM monitoring on the alleged present "need" to detect and prevent copyright infringement. It is also notable that in the context of the OPC's investigations into complaints under *PIPEDA* (which at present result only in non-binding recommendations) and in

⁷¹² L Ray Patterson, "Users' Rights in Copyright: An Interview with Ray Patterson" online: American Library Association, <<http://www.ala.org/ala/issuesadvocacy/copyright/copyrightarticle/usersrightscopyright.cfm>>. See also, Gervais, "The Price of Social Norms", *supra* note 49 at 44, n 17:

...many book and journal publishers were initially opposed to the introduction of photocopy machines in the 1970s. All or almost all publishers now license photocopying which has generated \$107.3 million of revenues in the U.S. in 2003, and \$250 million worldwide in so-called reprography fees and levies. That may not sound like a lot, but when one considers that it comes with no cost-of-sales, it is the rough equivalent of (assuming profits of 10% of gross revenues) \$2.5 billion in sales.

proceedings under *PIPEDA* before the Federal Court, an organization attempting to justify DRM monitoring may be the only entity presenting evidence to the OPC and the Court. The OPC and the Court may not have before them any competing or different perspectives or evidence, particularly in the case of an individual complainant.

Yet, despite the foregoing challenges and the fact that there is presently broad-based disagreement about whether alleged copyright infringement in the digital age has had a negative impact on copyright holders' interests (which, in any event, the OPC would arguably be ill-equipped to analyze and resolve in a specific *inter partes* case), under the current way that *PIPEDA* is applied, some organizations will likely be able to demonstrate a specific need—a specific history of copyright infringements—that will entitle them to claim under *PIPEDA* makes it appropriate for them to adopt a monitoring solution.

It should also be noted that the foregoing articulation of “need” presumes that copyright holders would define the “need” for DRM monitoring as being the detection and prevention of copyright infringement. That purpose is commonly invoked in support of the use of DRM and in support of providing legal protection for DRM. However, “need” might also be defined as the need to detect and prevent breaches of DRM licenses or the need to detect and prevent breaches of anti-circumvention laws (where such laws are enacted to protect DRM). In either case, in light of the exception to consent provided in section 7(1)(b), *PIPEDA* would arguably not even require consent for such collection of information.⁷¹³

Further, it is conceivable that copyright holders may define the “need” for DRM as being the control and exploitation of copyright works, including through the revenues that can be derived from the collection, use and disclosure of personal information through

⁷¹³ See *supra* note 671 and accompanying text.

DRM monitoring.⁷¹⁴ Defined in that manner, the need for DRM monitoring is directly linked to the purpose for the collection of personal information. However, what emerges is a use of DRM monitoring that is arguably disconnected, or at best indirectly connected, to copyright holders' rights and to the purposes and objectives of copyright.⁷¹⁵

2. Is monitoring likely to be effective in meeting the need?

Just as there is disagreement about whether there is a broad-based need for DRM monitoring, there is also disagreement about whether DRM monitoring is effective in protecting copyrighted works against infringement.⁷¹⁶ In addition to the technological challenges associated with "[f]inding more intrusive ways to track Internet usage,"⁷¹⁷ some suggest that DRM monitoring is not and

⁷¹⁴ See generally Chapter 3. See also Yochai Benkler, "Free as the air to common use: First Amendment Constraints on Enclosure of the Public Domain" (1999) 74 NYU L Rev 354 ("Video cassettes cannot ask you for your name and password every time you watch them, but a digital video disk or a movie downloaded 'on demand' can. [...] Digital technology thus offers copyright owners the hope that every single copy of their work will become its own tollbooth" at 422).

⁷¹⁵ See Part III of this chapter.

⁷¹⁶ Notwithstanding the OPC's findings in *PIPEDA* Case Summary #280, reconciling conflicting evidence about the effectiveness of DRM monitoring is, like the debate about whether there is a need for DRM monitoring, a matter which the OPC is arguably not well-positioned to determine. See *PIPEDA* Case Summary #280, *supra* note 677.

⁷¹⁷ Daniel Gervais, "User-Generated Content and Music File-Sharing: A Look at Some of the More Interesting Aspects of Bill C-32", in Geist, *Balanced Copyright*, *supra* note 63 at 447, 448:

Users empowered by social norms and ever-changing technological tools going well beyond peer-to-peer software, and even relying on the old USENET, circumvent technological protection measures (TPMs), and ultimately access millions of MP3s. Proxies and anonymous clients make the activity increasingly hard to detect and track. Finding more intrusive

cannot ever be effective.⁷¹⁸ Some copyright holders appear to conditionally agree with this conclusion, claiming that DRM monitoring will be ineffective if it is not protected by anti-circumvention laws: “[a]s no technological measure can permanently resist deliberate attacks, a TPM is only as good as its legal protection.”⁷¹⁹ The ineffectiveness of DRM in achieving copyright holders’ objectives may also be one of the reasons why many copyright holders who have experimented with DRM have more recently reduced or discontinued its use.⁷²⁰

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 circumstances, their DRM monitoring is effective. They may also be able to demonstrate that infringements declined or ceased following implementation of a DRM monitoring system. The court in *Eastmond* was persuaded by CPR’s evidence that no incidents had been reported since it had implemented its video surveillance system.⁷²¹

ways to track Internet usage is not just a technological challenge; it also pits copyright against other rights, including users’ privacy rights and interests. [footnotes omitted] [Gervais, “User-Generated Content”].

⁷¹⁸ See Peter Biddle, et al, “The Darknet and the Future of Content Distribution” in *Digital Rights Management* (Heidelberg: Springer, 2003) 155; Cory Doctorow, “Microsoft Research DRM Talk” (Presentation to Microsoft employees in Redmond, Washington (17 June 2004), online: Craphound.com <<http://craphound.com/msffdrm.txt>>. See also Richard Abbott “The Reality Of Modern File Sharing” (2009) 13 *Journal of Internet Law* 3.

⁷¹⁹ International Federation of the Phonographic Industry (IFPI), “The WIPO Treaties: Technological Measures” (March 2003), online: IFPI <<http://www.ifpi.org/content/library/wipotreaties-technical-measures.pdf>>.

⁷²⁰ See *supra* note 50 and accompanying text.

⁷²¹ *Eastmond*, *supra* note 69 at 179.

3. Is the loss of privacy proportional to the benefit gained?

Without detracting from the important observations expressed above under the first two elements of the *Eastmond* test, proportionality is likely the single most important and controversial element of the test in the context of DRM monitoring. This element raises important questions about the value of intellectual privacy and the objectives of copyright. Recall that in *Eastmond*, the OPC and the Federal Court considered relevant the fact that the cameras were in parking lots and other locations where there was a low *reasonable expectation of privacy*,⁷²² and that CPR had otherwise minimized the privacy impact of the cameras (including by not viewing the recordings unless incidents were reported).

The foregoing paragraph highlights a potential shortcoming of privacy laws, including the *Charter*, which utilize the concept of a ‘reasonable expectation of privacy.’ While this concept is not central in *PIPEDA*, which for the most part relies on a broad definition of personal information as opposed to expectations of privacy, the *Eastmond* case demonstrates that the notion of reasonable expectations of privacy can certainly creep into the analysis.⁷²³ As described below, this notion arguably weakens the

⁷²² *Ibid.* At paragraph 180, the Court stated that:

The Privacy Commissioner was of the view a person whose images might be recorded had a low expectation of privacy because the cameras were located to capture personal information in locations which were public places. I share his assessment. Generally, such a view accords with the thrust of the cases decided by the Supreme Court of Canada in section 8 *Charter* cases where an analysis of a reasonable expectation of privacy is weighed.

⁷²³ It is arguable that the reasonable expectation of privacy concept may leak into the *PIPEDA* analysis through subsection 5(3), which speaks of the “reasonable person”. For example, a court could find that deterring copyright infringement was a purpose that a reasonable person would consider appropriate in the circumstances, therefore suggesting that there is a reduced

protection for intellectual privacy that could be provided by the *Eastmond* test and *PIPEDA*.

Approaches to privacy that rely on a “reasonable expectation of privacy” can be problematic because, for example, technology, business practices, contracts and standard-form terms of service⁷²⁴ can sometimes be held to change or dictate the nature of individuals’ reasonable expectations.⁷²⁵ Chapter 3 includes discussion of a number of cases where courts have held that, in light of the wording of the standard terms of service of an ISP contract, individuals have a reduced expectation of privacy. The ‘reasonable expectation of privacy’ standard has its limitations and can risk the gradual erosion of intellectual privacy if applied in a non-normative manner:⁷²⁶

...if the state were free, at its sole discretion, to make
permanent electronic recordings of our private

reasonable expectation of privacy in respect of activities that relate to that purpose. I am indebted to Teresa Scassa for alerting me to this point.

⁷²⁴ See Chapter 3, Part II(D). See also *R v Cuttell*, 2009 ONCJ 471 where the Ontario Court of Justice agreed that a contractual agreement between the subscriber and ISP may relieve the ISP of its obligation to keep private information confidential. However, on the particular facts of the case, the court held that there was no evidence that the Bell Service Agreements in force during the relevant period were binding on the subscriber. Thus, the subscribers had a reasonable expectation of privacy in the information held by the ISP. In addition, in *York University v Bell Canada Enterprises* the court reinforced the view that the terms of service of an individual’s ISP can be a factor in determining whether the individual has a reasonable expectation of privacy in their internet usage. For example, the court reviewed the Bell and terms of service and held that: “A Bell customer can reasonably contemplate, therefore, that his or her identity may be disclosed by order of the court in the event he or she engages in unlawful, abusive or tortious activity.” *York University v Bell Canada Enterprises* 2009 CanLII 46447 (ON SC) at para 34.

⁷²⁵ See generally Shaun Spencer, “Reasonable Expectations and the Erosion of Privacy” (2002) 39 San Diego L Rev 843.

⁷²⁶ See Kerr & McGill, *supra* note 118.

communications, there would be no meaningful residuum to our right to live our lives free from surveillance. *The very efficacy of electronic surveillance is such that it has the potential, if left unregulated, to annihilate any expectation that our communications will remain private.*⁷²⁷

Intellectual privacy must therefore be a normative concept, not a (non-normative) concept that allows for changes in technology, contracting practices and standard form contracts, among other factors and practices, to determine the scope of intellectual privacy that we are entitled to.⁷²⁸ As Kerr and McGill point out in the criminal context:

[an approach to privacy that does not maintain a normative commitment to the concept] reduces our privacy expectations to little more than factual predictions about police behaviour and guesses about the kinds of technologies they are likely to employ. On this approach, [...] our privacy expectations are no longer about how police ought to behave, only about how they will behave. Such an approach eradicates the expectation of privacy from the realm of what is reasonable in a given situation, recasting it in light of that which is merely foreseeable in a particular set of circumstances. The emphasis is no longer on the individual and her or his right to be secure from unreasonable state intrusions, but instead concentrates on police action, relegating rights, at best, to an incidental consideration.⁷²⁹

Substituting “copyright holders” for “police” in the foregoing passage highlights how necessary it is that we maintain a

⁷²⁷ *R v Duarte*, *supra* note 135 at para 24 [emphasis added]. Quoted in *ibid.*

⁷²⁸ See generally Kerr & McGill, *supra* note 118.

⁷²⁹ *Ibid* at 420.

normative commitment to intellectual privacy in the copyright context. The state of DRM monitoring technology should not govern whether individuals have an expectation of intellectual privacy in their access to and enjoyment of copyright works.⁷³⁰ To the contrary, this dissertation argues that the values of intellectual privacy, including to the objectives of copyright, should require us to build a legal structure that preserves and protects those values in the face of monitoring technologies.⁷³¹

Similarly, intellectual privacy must avoid reductionism views that would reduce information about intellectual activities to isolated data (e.g. downloading a Madonna song), and thereby reduce the associated privacy value of the data.⁷³² We must maintain a holistic

⁷³⁰ See *R v Watts*, *supra* note 277:

To return to my original discussion, what I find difficult to believe is that the state of technology should govern whether there has been a breach of someone's privacy. It required an expert to give us the evidence that cordless phones could be intercepted. It is not, in my opinion, a matter that I could take judicial notice or that any average member of society would know. The only persons that would know would, I expect, be criminals and police officers with specialized training

⁷³¹ See Solove, "Conceptualizing Privacy", *supra* note 612 at 1143:

...privacy is not just found but constructed. By erecting a legal structure to protect the privacy of letters, our society shaped the practices of letter writing and using the postal system. It occurred because of the desire to make privacy an integral part of these practices rather than to pre-serve the status quo. [...] Therefore, determining what the law should protect as private depends upon a normative analysis, which requires us to examine the value of privacy in particular contexts. To do this, we must focus on our practices—specifically, the nature of privacy in these practices, the role that privacy plays in these practices, and the ends that these practices further.

⁷³² See generally Kerr & McGill, *supra* note 118 at 396:

[...] we warn against an excessively reductionist approach to informational privacy adopted in many recent reasonable

view of the context and of the social significance of intellectual activities and of the monitoring of those endeavours.⁷³³ For example, the context of DRM monitoring requires us to bear in mind the fact that copyright owners cannot obtain identity information from third parties except with a court order in order to associate individuals with particular works.⁷³⁴ Yet, similar information under current laws is easily obtained through a murky mix of standard form contracts and technology.

expectation of privacy cases. Once police activities are understood as nothing more than ‘capturing heat emanating from the wall of a building’ or ‘intercepting chemical emissions oozing through a backpack’, it is no longer possible to appreciate the deep social significance of RCMP planes beaming infrared lights at our homes in the middle of the night or police officers and their guard dogs randomly patrolling our high schools, bus stations and city streets.

⁷³³ See e.g. *R v AM*, *supra* note 142 at paras 39-40 [citing Kerr & McGill, *supra* note 118]:

It is in the nature of this rapidly developing field that *courts will need to return again and again to fundamental principles to draw the reasonableness line.*

Professor Kerr and Ms. McGill rightly warn of snooping technologies under development [...]. The s. 8 jurisprudence will continue to evolve as snooping technology advances. This flexibility is essentially what the “totality of the circumstances” approach is designed to achieve. On these occasions, critics usually refer to “Orwellian dimensions” and 1984, but the fact is that 1984 came and went without George Orwell’s fears being entirely realized, although he saw earlier than most the direction in which things might be heading. The Court can insist on proper evidence of what the police or government are up to and how, if at all, the information the police seek to collect can be used. As *Tessling* noted, “[w]hatever evolution occurs in future will have to be dealt with by the courts step by step. Concerns should be addressed with as they truly arise” (para. 55). [emphasis added].

⁷³⁴ See generally Chapter 3, Part II(D).

Transposing some of the foregoing to the DRM monitoring context, 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. Accordingly, it is conceivable that *PIPEDA*’s approach to the conflict between intellectual privacy and copyright in such cases may result in DRM monitoring practices being considered proportionate to the diminishment of intellectual privacy.

However, from within a copyright perspective, and with reference to the broader set of values that are interrelated with intellectual privacy as described in Chapter 2, there would be good reasons to reject distinctions between various forms of copyrighted works when it comes to the application of the *Eastmond* test. Taking into account the purposes of copyright and the values of intellectual privacy suggests that 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 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, for example, offers the following view:

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.

Rock offers the possibility of a relation which is intense, strong, alive, "dramatic" (in that rock presents itself as a spectacle, that listening to it is an event and that it produces itself on stage), with a music that is itself

impoverished, but through which the listener affirms himself...⁷³⁵

Is the loss of intellectual privacy proportional to the benefit gained in the case DRM monitoring? This is a difficult question. 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 issues at play.

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 such monitoring being found proportional under *PIPEDA*. 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 found under *PIPEDA* to be proportional to the benefit gained by DRM monitoring.

Significantly, the foregoing proportionality analysis fails to take into account the adverse effects that DRM monitoring has on the very purposes of copyright. For example, if the objectives of copyright or creative output were to suffer as a result of DRM monitoring and the resulting diminishment of intellectual privacy (as is argued in this dissertation),⁷³⁶ notwithstanding that many individual copyright holders might be better off using DRM monitoring, it would seem only natural that the adverse impact of

⁷³⁵ Michel Foucault & Pierre Boulez, “Contemporary Music and the Public”, translated by John Rahn (1985) 24 *Perspectives of New Music* 6.

⁷³⁶ See also Cohen, “Information Rights”, *supra* note 652 at 11:

...the imposition of metered usage requirements will significantly change the creative process, both by imposing cost constraints and by reducing serendipitous discovery and browsing. As reading patterns change to accommodate metering, both the volume and diversity of creative output may suffer gradual attrition.

the DRM monitoring on the overall purposes of copyright should be taken into consideration. Unfortunately, that is not the way that the proportionality analysis, or *PIPEDA* in general, operates. As the Federal Court has held,⁷³⁷ *PIPEDA* is intended to facilitate the flow of personal information by balancing privacy against organizations' need to collect, use and disclose information on a case by case basis. There is considerable doubt about whether a *PIPEDA*-like model of regulation can save intellectual privacy, let alone copyright.

4. 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 the court in *Eastmond* held that organizations are entitled to reject less privacy invasive alternatives if they are, for example, more costly, alternatives must be properly considered.

In the case of DRM monitoring, there do appear to be less privacy-invasive ways of achieving the same end (assuming that the "end" is protecting against infringement and facilitating remuneration for rights holders); there is no inherent reason why DRM monitoring is needed at all,⁷³⁸ let alone any reason why it must be privacy-invasive. A number of commentators have noted that DRM design need not involve constant monitoring or the collection of personal information.⁷³⁹ Indeed, Lessig agrees with Cohen that the benefits

⁷³⁷ *Englander v TELUS*, *supra* note 209 at paras 38, 46.

⁷³⁸ See Part III of this chapter.

⁷³⁹ See e.g. Stefan Bechtold, "Value-Centered Design of Digital Rights Management – Perspectives on Emerging Scholarship" (2004), 1 INDICARE Monitor, online: INDICARE <http://www.indicare.org/tiki-read_article.php?articleId=39>. For a discussion of such proposals, see generally Cameron, "Infusing Privacy Norms in DRM", *supra* note 28; Kerr, "If Left to their own Devices", *supra* note 28; Mulligan & Burstein, *supra* note 337.

of monitoring need not involve a diminishment of intellectual privacy:

All of the good that comes from monitoring could be achieved while protecting privacy. It may take a bit more coding to build in routines for breaking traceability; it may take more planning to ensure that privacy is protected. But if those rules are embedded intellectual property up front, the cost would not be terribly high. It is far cheaper to architect privacy protections now rather than retrofit for them later.⁷⁴⁰

Ensuring that individuals are authorized to access or use particular content, which is a central purpose of DRM, does not necessarily require monitoring or the collection of personal information. If this premise is accepted, such alternative solutions may render privacy-invasive DRM inappropriate in many cases under the *Eastmond* test.

C. Conclusions

The preceding sections of this chapter have considered the application of data protection law to DRM monitoring practices. This jurisprudence is important for several reasons. For example, in the absence of the adoption of a model of statutory reform proposed in this dissertation, data protection laws will be influential in shaping the future course of intellectual privacy. 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. Unfortunately, as suggested above, *PIPEDA* may facilitate or be ill-equipped to address DRM monitoring practices which undermine intellectual privacy and the objectives of copyright. Courts and regulators

⁷⁴⁰ Lessig, *Code version 2.0*, *supra* note 24 at 197.

applying privacy laws of general application to the conflicts between copyright and intellectual privacy are not well-placed to make the difficult and far reaching policy choices that are at stake at the nexus between copyright and intellectual privacy.

In addition, as mentioned at the outset of this part, the foregoing analysis under data protection law is also suggestive of possible questions that copyright might ask itself in designing rules for addressing intellectual privacy within copyright. For example, one might ask if a *PIPEDA*-like model should be adopted and adapted for use in addressing intellectual privacy in the *Copyright Act*. As suggested in some of the analysis in this chapter, however, under data protection law there may be something of a disconnect 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 and *PIPEDA* 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—the *Eastmond* test would fail to adequately recognize the biographical nature of information about individuals’ access to and use of copyright works, and the potentially invasive profiling and diminishment of intellectual privacy that can result from monitoring individuals’ activities in that context. Austin puts an aspect of 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.⁷⁴¹

Yet, even with the robust definition of intellectual privacy proffered in Chapter 2 of this dissertation, as described above, the *Eastmond* test in particular and *PIPEDA* in general are arguably insufficient and ill-equipped to address the conflicts between copyright and intellectual privacy. Leaving intellectual privacy to be determined on a case-by-case basis under the *PIPEDA* regime asks far too much of the *PIPEDA* and the OPC and risks too much, for both copyright and intellectual privacy. In addition, it appears likely that *PIPEDA* would *facilitate* many DRM monitoring practices with adverse effects for both copyright objectives and for intellectual privacy.⁷⁴² For these reasons and the reasons described in Chapter 4 (for why copyright can and should account for intellectual privacy), the conflicts between copyright and intellectual privacy should be addressed in copyright and should not be left to data protection laws such as *PIPEDA*. This is a view shared by Bygrave and Koelman:

⁷⁴¹ Austin, *supra* note 670 at 214.

⁷⁴² There are also other reasons to doubt the adequacy of the response that a *PIPEDA* model could provide to the conflicts between copyright and intellectual privacy. For example, although the Federal Court has recently issued several decisions under *PIPEDA* which include modest damage awards (e.g. *Girao v. Zarek Taylor Grossman Hanrahan LLP*, 2011 FC 1070), *PIPEDA* “leaves the Privacy Commissioner of Canada without order-making powers to carry out sanctions in any manner proportional to the damage that will be done by DRM and other online privacy-invasive technologies.” Kerr, “If Left to their own Devices”, *supra* note 42 at 179, n 48. As discussed in Chapter 2, it should also be noted that *PIPEDA* applies only to *commercial* activities that involve the collection, use or disclosure of personal information.

Whereas the relationship between copyright and privacy is a problem with broad implications [for example, as articulated by Cohen and as discussed in Chapters 1 through 3 of this dissertation], and whereas user privacy and autonomy may be viewed as already addressed in copyright law [for some of the reasons discussed in Chapter 4 of this dissertation], *the extent to which the users' private sphere may be invaded while enforcing copyrights through [DRM systems] should arguably not be left to a general regulatory instrument like the Data Protection Directive, but should be addressed more explicitly in copyright law.*⁷⁴³

In addition to demonstrating that conflicts between copyright and intellectual privacy should not be left to data protection laws or other similar rules, the foregoing analysis under *PIPEDA* highlights the need for Parliament, not privacy regulators and not the courts, to grasp the nettle. Accounting for intellectual privacy in copyright is not a matter which should be addressed on a case-by-case basis. The choices at stake are not only complex but have potentially far-reaching ramifications for both copyright and intellectual privacy. This conclusion is consistent with the traditional view in Canada that Parliament, not the judiciary, is best positioned to reconcile competing policy considerations where major reforms to the law are at issue. McLachlin, J. (as she was then) explains this principle in *Watkins v Olafson*:

The court may not be in the best position to assess the deficiencies of the existing law, much less problems which may be associated with the changes it might make. The court has before it a single case; major changes in the law should be predicated on a wider view of how the rule will operate in the broad generality of cases. Moreover, the court may not be in a

⁷⁴³ Bygrave & Koelman, "Privacy, Data Protection and Copyright", *supra* note 61 at 51 [emphasis added] [footnotes omitted].

position to appreciate fully the economic and policy issues underlying the choice it is asked to make. Major changes to the law often involve devising subsidiary rules and procedures relevant to their implementation, a task which is better accomplished through consultation between courts and practitioners than by judicial decree. Finally, and perhaps most importantly, there is the long-established principle that in a constitutional democracy it is the legislature, as the elected branch of government, which should assume the major responsibility for law reform... Considerations such as these suggest that major revisions of the law are best left to the legislature.⁷⁴⁴

With the foregoing in mind, this chapter next turns to some of the recent proposals for statutory reform in Canada which in different ways touch on the conflicts between copyright and intellectual privacy as described in Chapter 3.

II. Recent Proposals for Statutory Reform

A. Levies Redux

Concurrent with the recent resurgence of questions about individuals' intellectual privacy interests in relation to their access to and use of copyright works, the topic of levies and collectives has again come to prominence, just as it did in the 1960s as described in Chapter 4.⁷⁴⁵ Over roughly the past decade, a number

⁷⁴⁴ *Watkins v Olafson*, [1989] 2 SCR 750 at para 14 [emphasis added].

⁷⁴⁵ Mihaly Ficsor, "Collective Management of Copyright and Related Rights at a Triple Crossroads: Should it Remain Voluntary or may it be "Extended" or Made Mandatory?" (October 2003), online: UNESCO <http://portal.unesco.org/culture/en/files/14935/10657988721Ficsor_Eng.pdf> at 1:

of proposals have been made for the adoption of levy schemes in digital copyright, including in Canada.⁷⁴⁶ Indeed, with digital copyright issues and copyright reform in a tumultuous state by 2008, the headline in Canada exclaimed “Everybody is jumping on the levy bandwagon.”⁷⁴⁷

Respect for intellectual privacy is among the prominent benefits touted in connection with levy regimes:⁷⁴⁸ “with one payment, consumers have free access and uncontrolled options for easy private uses with no monitoring of use.”⁷⁴⁹ Indeed, although collective management of copyright comes with its own unique

In the case of a traditional, fully fledged collective management system, the right owners authorize collective management organizations to monitor the use of their works, to negotiate with prospective users, to grant them licenses under certain conditions and on the basis of a tariff system, to collect the remuneration, and to distribute it among the owners of rights. Many elements of the management of rights in that type of system are standardized – in fact, they may even be “collectivized”: the same tariffs, the same licensing conditions and the same distribution rules may apply to all works which belong to a given category; sometimes social and/or “cultural” deductions are also made, etc.

⁷⁴⁶ See e.g. Neil Weinstock Netanel, “Impose a Noncommercial Use Levy to Allow Free Peer-to-Peer File Sharing” (2003) 17 Harv JL & Tech 1; William Fisher, *Promises to Keep: Technology, Law, and the Future of Entertainment* (Palo Alto: Stanford University Press, 2004); Gervais, “User-Generated Content”, *supra* note 717.

⁷⁴⁷ Michael Geist, “Everybody is jumping on the levy bandwagon” *Toronto Star* (10 March 2008), online: *Toronto Star* <<http://www.thestar.com/sciencetech/article/326749>>.

⁷⁴⁸ Gervais, “User-Generated Content”, *supra* note 717 (“If privacy-invasive tools are used to distribute and/or monitor end-users, privacy will be(come) a major issue. If, however, systems that decouple usage data from individual identities early on (upstream) are used, then the issue may vanish from major policy radars” at 471).

⁷⁴⁹ Helberger et al, “INDICARE 2004”, *supra* note 31 at 25.

complexities and challenges for a variety of non-privacy reasons,⁷⁵⁰ (which perhaps explain why it has not enjoyed more uptake in the digital era), it presents a powerful potential model for respecting individuals' intellectual privacy interests while at the same time ensuring that economic incentives exist for the creation of copyright works.⁷⁵¹ Gervais summarizes some of the key points as follows:

From the users' standpoint, collectivization [...] offers important advantages. In fact, it may be essential to the preservation of their intellectual privacy. Of the three potential types of players previously surveyed (ISPs, copyright collectives, and new technology companies), copyright collectives may offer a slightly higher degree of comfort. In most cases, these entities are non-profit and have a long history of maintaining user anonymity by aggregation of usage data they perform in order to distribute funds to appropriate rightsholders. To put it differently, they have demonstrated an ability to decouple users from usage data. [...]

From the point of view of users, however, the question of the protection of the anonymity of usage data is

⁷⁵⁰ See generally, Daniel J Gervais. "The Landscape of Collective Management Schemes" (2011) 34 Colum-VLA J L & Arts 423; Daniel J Gervais, "A Uniquely Canadian Institution: The Copyright Board of Canada" in Ysolde Gendreau, ed, *An Emerging Intellectual Property Paradigm* (Cheltenham: Edward Elgar, 2008) ("collective management is not a panacea, and questions have been raised about the efficiency and the transparency of [collective management organizations] and their continued relevancy in the digital age" at abstract).

⁷⁵¹ Boyle characterizes such solutions as "alternative methods of encouraging cultural production while maximizing technological and cultural freedom." James Boyle, *The Public Domain: Enclosing the Commons of the Mind* (New Haven: Yale University Press, 2008) at 271.

based on what seems a questionable assumption, namely that usage data *should be captured at all*.⁷⁵²

While a review and analysis of collective management is beyond the scope of this dissertation,⁷⁵³ it must be acknowledged that it presents a potential alternative solution to some of the conflicts between copyright and intellectual privacy described herein. In theory, at least, levy systems could give individuals a wide berth to engage with creative works anonymously or in private.

B. Proposed Amendments to the Copyright Act

As discussed in Part II of Chapter 3, over roughly the past decade, Canada has on several occasions considered potential amendments to the *Copyright Act* that would, among other things, provide legal protections for DRM technologies in the form of anti-circumvention and anti-device rules. This section briefly reviews the privacy-related components these proposals.

The first iteration of such proposed rules was tabled in June 2005 in the form of Bill C-60. As highlighted in Chapters 1 and 3, Bill C-60 was criticized for its total failure to address intellectual privacy,⁷⁵⁴

⁷⁵² Gervais, “The Price of Social Norms”, *supra* note 49 at 66 [emphasis in the original].

⁷⁵³ For further discussion, see *supra* note 750 and accompanying text.

⁷⁵⁴ See e.g. Kerr, “If Left to their own Devices”, *supra* note 42 at 170:

When it comes to protecting intellectual privacy — a core value underlying the doctrine of intellectual property — the recently released Bill C-60 whispers with the sounds of silence. Although ample statutory language is offered to illustrate how the law will protect technological protection measures (TPMs) from people, the Bill offers zero protection to people from TPMs.

It is my contention that statutory silence about the permissible scope of use for TPMs risks too much from a privacy perspective. In particular, I am of the view that any law protecting the surveillance technologies used to enforce

despite the fact that at least one of the policy papers commissioner by Industry Canada expressly recommended that privacy be taken into consideration: “[i]n order to protect privacy in lawful use, copyright protection should not extend to what is often referred to as the integrity of a rights management system, such as subsystems that allow rights holders to track the (individual) use of copyright material.”⁷⁵⁵

In late 2005, Bill C-60 died on the order paper as a result of the dissolution of Parliament. However, it appears that lawmakers in Canada paid some attention to the privacy-related criticisms that had been leveled against Bill C-60. In three subsequent bills introduced to amend the *Copyright Act*, the first⁷⁵⁶ and second⁷⁵⁷ of which died on the order paper and the third⁷⁵⁸ of which is currently pending before Parliament at the time of writing, the government introduced proposed amendments which included a privacy-related defence to the proposed prohibition on circumventing TPMs. The language of the proposed amendments was identical in the three bills and reads as follows:

41.14 (1) [The prohibition against circumventing a technological protection measure] does not apply to a person who circumvents a technological measure if

copyright must also contain express provisions and penalties that protect citizens from organizations using those TPMs to engage in excessive monitoring or the piracy of personal information.

⁷⁵⁵ Marcel Boyer, “Authors, Makers, Photographers and Publishers in Canada: A Report for Industry Canada” (2003), online: Industry Canada <http://www.ic.gc.ca/eic/site/ippd-dppi.nsf/eng/h_ip01073.html> at 4. See also Kerr, Maurushat & Tacit, “TPMs Part I”, *supra* note 32; Kerr, Maurushat & Tacit, “TPMs Part II”, *supra* note 32.

⁷⁵⁶ Bill C-61, *supra* note 420.

⁷⁵⁷ Bill C-32, *An Act to Amend the Copyright Act*, 3rd Sess, 40th Parl, 2010 [Bill C-32].

⁷⁵⁸ Bill C-11, *An Act to Amend the Copyright Act*, 1st Sess, 41st Parl, 2011 [Bill C-11].

- (a) the work, performer's performance fixed in a sound recording or sound recording that is protected by the technological measure is not accompanied by a notice indicating that its use will permit a third party to collect and communicate personal information relating to the user or, in the case where it is accompanied by such a notice, the user is not provided with the option to prevent the collection and communication of personal information without the user's use of it being restricted; and
- (b) the only purpose of circumventing the technological measure is to verify whether it permits the collection or communication of personal information and, if it does, to prevent it.

The same section also created a privacy exception to the prohibition on circumvention devices:

- (2) [The prohibition against offering services, etc. and manufacturing, distributing, etc. devices primarily for circumventing technological protection measures] do not apply to a person who offers services to the public or provides services, or manufactures, imports or provides a technology, device or component, for the purposes of circumventing a technological measure in accordance with subsection (1), to the extent that the services, technology, device or component do not unduly impair the technological measure.

In the government's clause-by-clause analysis of Bill C-32, the rationale for the above provisions was described as follows, with reference to the Sony BMG controversy described in Chapter 3:

[t]his exception addresses situations such as those created by the Sony BMG TPM which was included on certain CDs. The TPM communicated personal

information from consumers' computers to Sony BMG—without providing an option for consumers to prevent such disclosure. This exception would ensure that a person could circumvent such a TPM.⁷⁵⁹

Although it is argued Part III that the foregoing proposed privacy-related provisions in the *Copyright Act* do not go nearly far enough to address intellectual privacy, it must be acknowledged that the provisions represent a significant development in the history of Canadian copyright law and unquestionably signal that lawmakers in Canada are open to including in *copyright law* the sort of provisions that this dissertation argues are essential for the protection of intellectual privacy.

It should be noted that the proposed amendments above do not include a privacy-based exception in respect of the proposed prohibition against the removal of RMI.⁷⁶⁰ As in the case of the

⁷⁵⁹ The government's analysis was obtained by Michael Geist pursuant to an access to information request. Michael Geist, "Behind the Scenes of Bill C-32: Govt's Clause-By-Clause Analysis Raises Constitutional Questions" (27 September 2011), online: MichaelGeist.ca <<http://www.michaelgeist.ca/content/view/6026/125/>>.

⁷⁶⁰ The proposed prohibition is found in section 41.22:

41.22 (1) No person shall knowingly remove or alter any rights management information in electronic form without the consent of the owner of the copyright in the work, the performer's performance or the sound recording, if the person knows or should have known that the removal or alteration will facilitate or conceal any infringement of the owner's copyright or adversely affect the owner's right to remuneration under section 19. [...]

(4) In this section, "rights management information" means information that

(a) is attached to or embodied in a copy of a work, a performer's performance fixed in a sound recording or a sound recording, or appears in connection with its communication to the public by telecommunication; and

failure of Bill C-60 to address privacy at all, the absence of this exception is curious given that the privacy-related ramifications of RMI were expressly raised in a paper commissioned by the government, including a suggestion that individuals should be entitled to remove such information:

The collection and commercialization of tracking information is a matter of concern because it may violate users' privacy. If one accepts the view that the protection of privacy is a concern that trumps economic considerations then, clearly, one should allow the removal of such RMI. [...]

Should one conclude therefore that users must be allowed to remove tracking information? A risk one must pay heed to is that removal of tracking codes could lead -either by mistake or by design -to the removal of other information. *A preferred approach is to require that the parties who embed tracking codes inform users that utilization of a work is monitored or could be monitored, and demand that these parties provide users with a very simple way to disable the tracking mechanism. Absence of such mechanism should be sufficient to allow the removal or disabling of tracking information.*⁷⁶¹

(b) identifies or permits the identification of the work or its author, the performance or its performer, the sound recording or its maker or the holder of any rights in the work, the performance or the sound recording, or concerns the terms or conditions of the work's, performance's or sound recording's use. [emphasis added]

⁷⁶¹ Abraham Hollander, "Assessing Economic Impacts of Copyright Reform on Selected Users and Consumers: Prepared for Marketplace Framework Policy Branch, Industry Canada", online: Industry Canada <<http://www.ic.gc.ca/eic/site/ippd-dppi.nsf/eng/ip01188.html>> [emphasis added]. Hollander also notes that:

When sellers embed tracking information they are in fact offering a tied exchange, a form of barter. They propose a

Of course, the suggestion in the foregoing passage that individuals be notified and provided with an 'opt-out' is similar to what was ultimately adopted in the anti-circumvention provision of Bill C-11 as described above.⁷⁶²

III. Imagining Intellectual Privacy Rules in Copyright Reform Statutes

Articulating legal principles for protecting the intellectual privacy interests implicated by DRM technologies is far more complicated than articulating the normative case for such protection. Normative theories are more supple than legal ones, which tend to move cautiously along well-trodden paths. Developing a legal theory of intellectual privacy for the information age requires an act of legal imagination.

– Julie Cohen⁷⁶³

Given the capabilities of DRM and other emerging technologies, as bolstered by standard-form contracts, accounting for intellectual privacy in contemporary copyright is a complex exercise, requiring, among other things, an assessment of the appropriate bounds of control that copyright holders ought to have over copyright works and in particular over individuals' private use of such works.

product in exchange of money and tracking information. One must assume that such tying increases the value of the transaction to the seller, i.e. the party imposing the bundle. This does not entail, however, that tracking information also produces more value for buyers. And, when buyers lose more than sellers gain, there is a loss in economic efficiency. From an economic perspective then, there is no apparent reason to protect tracking information.

⁷⁶² See *supra* note 758 and accompanying text.

⁷⁶³ Cohen, "DRM and Privacy", *supra* note 3 at § III.

The first point to bear in mind in thinking about how copyright ought to account for intellectual privacy is that diminishing intellectual privacy does not fit under copyright's bundle-of-rights paradigm. The absurdity of the phrase 'the exclusive right to diminish intellectual privacy' or even 'the exclusive right to increased access to personal information of those who access materials subject to copyright' reinforces how inappropriate it is to think in such terms. It also serves to highlight the fact that, notwithstanding the nexus between copyright and intellectual privacy, the diminishment of intellectual privacy in association with copyright works is not encompassed within the normal exploitation of a work under copyright law.⁷⁶⁴

If there is to be any diminishment of intellectual privacy in association with copyright works, it must *at a minimum* be instrumental in fulfilling the goals of copyright. In other words, if there is to be any diminishment of intellectual privacy by copyright holders, there must be a sufficient copyright-based justification for it. This is easier said than measured. In a similar vein, the *PIPEDA* analysis in Part I of this chapter demonstrates how difficult it can be to assess whether a practice that diminishes intellectual privacy is reasonable, particularly in respect of DRM monitoring.

The foregoing suggests that copyright should, by default, avoid conflict with intellectual privacy at all times. This is a concept which is arguably consistent with the limitation and necessity principles in *PIPEDA*,⁷⁶⁵ the surveillance-related jurisprudence examined in Part I of this chapter, and the need to identify specific purposes and obtain consent for the collection of information. Bailey has articulated a similar view with respect to freedom of

⁷⁶⁴ This point is consistent with the assertion made by some commentators that anti-circumvention and anti-device laws are 'paracopyright' laws. See e.g. deBeer, "Constitutional Jurisdiction Over Paracopyright Laws", *supra* note 393.

⁷⁶⁵ *PIPEDA*, *supra* note 13, Principles 4.4 and 4.4.1.

expression values, noting also that any limitations on expressive rights must be limited and tied to the purposes of copyright:

Parliament has the opportunity, and the obligation, to chart a course that compromises the entrenched expressive rights of users in favour of the economic interests of copyright holders only insofar as is necessary to serve the public interest in a robust marketplace of ideas.⁷⁶⁶

However, the above does not mean that intellectual privacy must be paramount and absolute when it conflicts with copyright. There will be limited cases where copyright will be justified in permitting the diminishment of intellectual privacy where absolutely necessary. It is expected that such cases should be few and far between. By default, copyright should always be looking for ways to achieve its ends without diminishing intellectual privacy.

The default principle enunciated in the forgoing paragraphs is one of the most important principles missing in Bill C-11 to date. Bill C-11 and its predecessors *presume* that copyright holders will, by *default*, collect personal information from individuals and otherwise diminish their intellectual privacy in connection with copyright works. Bill C-11 does not place any positive obligations on copyright holders to take the steps contemplated in section 41.14. Indeed, in that section, Bill C-11 provides only what appears to be a mild disincentive to diminish intellectual privacy, if it is a disincentive at all. The only consequence of a diminishment of intellectual privacy (as contemplated by Bill C-11) is that the affected individual would have a *defence* to the prohibition against circumventing TPMs in certain cases. There are a number of problems and shortcomings with this approach. For starters, as the Canadian Bar Association and others have pointed out, individuals have neither the expertise nor the means to circumvent TPMs and,

⁷⁶⁶ Bailey, “Deflating the Michelin Man”, *supra* note 655 at 166.

in addition, under Bill C-11 individuals are effectively denied the devices they would need to circumvent:

The efficacy of [section 41.14] is questionable because individuals will typically not have the knowledge or means to circumvent TPMs for the purpose of protecting their privacy. Individuals will require technical assistance to enable them to do so. Although proposed s. 41.14(2) contains an exception for those who provide technical assistance to enable circumvention for the protection of privacy, again, whether individuals will be able to make use of the exception is questionable. The exception is available only 'to the extent that the services, technology, device or component do not unduly impair the technological protection measure.' Once most technological measures are circumvented, the protected content will be in the clear. In other words, it is difficult to conceive of a service or device that would permit circumvention of a TPM for the purpose of protecting privacy but would not unduly impair the TPM.⁷⁶⁷

⁷⁶⁷ Canadian Bar Association (CBA), "Submission on Bill C-32, *Copyright Modernization Act*", (February 2011), online: CBA <<http://www.cba.org/cba/submissions/pdf/11-06-eng.pdf>> at 11. The author was a member of the Copyright Working Group for the National Intellectual Property and Privacy and Access Law Sections of the Canadian Bar Association which prepared this submission. See also Michael Geist, "Setting the Record Straight: 32 Questions and Answers on C-32's Digital Lock Provisions" (June 2010) at 9, online: MichaelGeist.ca <http://www.michaelgeist.ca/component/option,com_docman/task,doc_download/gid,32/>:

[section 41.14] fails to provide Canadians with full privacy protection and Bill C-32 unquestionably makes it more difficult for Canadians to effectively protect their privacy. The reason for this is that though there is an exception that permits circumvention to protect (and prevent the collection or communication of) personal information, the ability to exercise this exception is rendered difficult by virtue of the inability to

To the above, it should be added that the proposed defence to a breach of the anti-circumvention provision in Bill C-11 is troubling because it is only relevant in circumstances where the copyright holder has *already* violated the spirit of Bill C-11 (and *PIPEDA*) by collecting information without adequate consent and without providing consumers with an opt-out. It is risible to suggest that the only remedy for an individual whose intellectual privacy has been violated by DRM monitoring (which as argued herein should be prohibited or restricted by copyright law in the first place) is that the individual has to (a) invest time and resources in figuring out *how* to circumvent the offending DRM technology and (b) if they are able to circumvent, assume the risk in so doing that their conduct may nevertheless run afoul of the anti-circumvention prohibition, since their only right under Bill C-11 is to exercise a *defence* to the anti-circumvention prohibitions under the *Copyright Act*.

With these observations and principles in mind, the passages below provide five basic recommendations for rules to mitigate intellectual privacy issues within copyright in Canada.

1. Place clear and affirmative obligations on copyright holders in respect of intellectual privacy

For the reasons set forth above, the set of rules in Bill C-11 will not protect or produce conditions of respect for intellectual privacy within copyright. When it comes to addressing intellectual privacy,

legally obtain devices (i.e. software programs) for this very purpose. [...]

In other words, you can use a circumvention device to protect your privacy but it cannot allow you to simultaneously access the underlying content. Of course, once most circumvention devices circumvent a technological measure, the protected content will be in the clear. Distribution of this form of device is therefore illegal. Moreover, service providers will be likely be unwilling to use this provision for fear of facing liability.

noting is required of copyright holders under Bill C-11 and too much is expected of individuals.⁷⁶⁸ The rules in the *Copyright Act* must place *affirmative* obligations on copyright holders to do the kinds of things contemplated in section 41.14 of Bill C-11 and the further concepts suggested below.

The starting point for the analysis in each case should be that, by *default*, copyright holders should not engage in practices which diminish intellectual privacy. For example, collecting, using or disclosing personal information will rarely, if ever, be necessary for the exercise of copyright holders' rights. Such practices must only be adopted when doing so furthers the goal of copyright law or for some other appropriate related purpose,⁷⁶⁹ and only when the requirements in the next paragraph are satisfied.

Individuals must be given prominent and effective notice of practices which implicate intellectual privacy (as described below) and a straightforward means to opt-out of DRM practices which diminish their intellectual privacy, while at the same time retaining the right and ability to access the works anonymously or in private.⁷⁷⁰ Interestingly, even in its current form, Bill C-11 appears to contemplate that individuals should be able to access works anonymously, though it falls short in the implementation. In addition to the right of individuals under Bill C-11 to circumvent the DRM systems of copyright holders who fail to follow the *suggestions* contained in section 41.14 (which this dissertation suggests should be converted to *requirements*), there must also be real consequences for copyright holders who fail to comply with the affirmative obligations proposed in this part, as discussed below.

⁷⁶⁸ At least under *PIPEDA* an individual need only file a complaint and the OPC essentially takes it from there.

⁷⁶⁹ See Part IV of Chapter 2.

⁷⁷⁰ For a discussion of the anonymity principle, see Kerr, "If Left to their own Devices", *supra* note 42.

2. Address standard-form contracts

Perhaps the biggest area where copyright could take steps to preserve the private sphere of individual use of copyright works, and thereby minimize its impact on intellectual privacy, is in the area of contracting.⁷⁷¹ Standard form contracts, implemented through DRM, are not only the biggest threat to individuals' fair use rights but also to their informational and intellectual privacy rights as discussed in Chapter 3. Contracts are a problem from a copyright perspective because they can eviscerate individuals' private use rights that might otherwise be provided for either by fair dealing in copyright or by ownership of a tangible copy of a work. Apart from considerations about whether such contracts are enforceable from a data protection perspective, restricting or prohibiting the ability of copyright holders to contract individuals out of fair dealing rights could go a long way to preserving a private sphere of individual privacy in relation to copyright works (i.e. intellectual privacy). In addition, in the context of the Parliamentary review of *PIPEDA*, Kerr has suggested that the following measures be adopted in respect of the use of standard form contracts (which, in addition to providing options for

⁷⁷¹ See generally Dr. Ian Kerr, Canada Research Chair in Ethics, Law and Technology, University of Ottawa, "Submission to The House of Commons Standing Committee on Access to Information, Privacy and Ethics on The Personal Information Protection and Electronic Documents Act ("PIPEDA")", online: [On the Identity Trail <http://www.idtrail.org/files/ik_pipeda_review_submission_final_formatte d.pdf>](http://www.idtrail.org/files/ik_pipeda_review_submission_final_formatte d.pdf). See also Dr. Ian Kerr, Canada Research Chair in Ethics, Law and Technology, University of Ottawa, As an Individual (Testimony delivered at the Standing Committee on Access to Information, Privacy and Ethics, December 11, 2006), online: [Parliament of Canada <http://www.parl.gc.ca/HousePublications/Publication.aspx?DocId=2600931&Language=E&Mode=1>](http://www.parl.gc.ca/HousePublications/Publication.aspx?DocId=2600931&Language=E&Mode=1) ("My testimony today, however, will be to suggest that there is a much bigger threat to privacy that comes from a much more primitive and much more basic technology. [...] In English, we call it the standard form contract").

inclusion in copyright law, would help address some of the shortcomings of *PIPEDA* discussed earlier in this chapter):

- stipulate that the existence of a contract claiming to permit personal information collection has no evidentiary relevance to a determination of the purported reasonableness or appropriateness of its collection, use and disclosure practices
- stipulate a series of conditions under which contracts requiring an individual to contract out of privacy protections provided for in *PIPEDA* shall not be enforceable
- stipulate that organizations may not prohibit an individual from withdrawing consent to the collection, use or disclosure of personal information related to the individual
- provides the Privacy Commissioner (or an associated Tribunal) with ordermaking powers, including the power to award damages.⁷⁷²

But, how are we to determine “what conditions should be necessary for an effective waiver of intellectual privacy if protection for intellectual privacy is to be meaningful”?⁷⁷³ In addition to the foregoing recommendations from Kerr, which I support, there are a number of additional observations regarding the elements that should be considered for inclusion in copyright rules designed to address intellectual privacy. In this respect, *CASL*⁷⁷⁴ is an extremely useful reference model for the sorts of rules that might be included in copyright, because, as discussed in Chapter 2, *CASL* targets

⁷⁷² *Ibid* at 3.

⁷⁷³ Cohen, “DRM and Privacy”, *supra* note 3.

⁷⁷⁴ *CASL*, *supra* note 220.

activities which are similar or identical to DRM monitoring in many cases.⁷⁷⁵

Indeed, *CASL* is informative about the kinds of requirements that may be imposed on copyright holders who utilize DRM systems which collect personal information. Under *CASL*, for any program that collects personal information, the owner must “clearly and prominently” and “separately and apart from the licence agreement,” “describe the program’s material elements that perform the function or functions, including the nature and purpose of those elements and their reasonably foreseeable impact on the operation of the computer system.”⁷⁷⁶ This approach would be appropriate to adopt in the copyright context as well, since many DRM systems would meet the requirements under *CASL* for the heightened level of notice and consent just described.⁷⁷⁷ A consistent approach could be taken in the *Copyright Act*.

3. Implement meaningful penalties and enforcement in respect of intellectual privacy

The penalties and enforcement mechanisms under *CASL* demonstrate potential approaches that could be integrated into copyright’s approach to intellectual privacy. The multiple enforcement channels in *CASL* provide a number of options for consideration: private right of action, regulatory investigations and undertakings, and significant administrative monetary penalties.⁷⁷⁸ In order for any copyright rules respecting intellectual privacy to be

⁷⁷⁵ *CASL* is discussed in Chapter 2, Part II(C).

⁷⁷⁶ *Ibid*, s 10(4).

⁷⁷⁷ Indeed, the Sony rootkit DRM system was classified as “spyware” that would certainly have been captured by *CASL*. See *supra* notes 362, 366-368, 759 and accompanying text.

⁷⁷⁸ For a general discussion of *CASL*, see Kris Klein & Shaun Brown, *A Complete Guide to e-Marketing under Canada’s Anti-Spam Legislation* (Toronto: Carswell, 2011).

effective, it is likely that the rules will need some ‘teeth’. With reference to the powers and penalties under *CASL*, the OPC has in recent times suggested that under *PIPEDA* it may be time that she name organizations who violate *PIPEDA* and that she should be given order-making power and the power to impose administrative monetary penalties.⁷⁷⁹ Each of these developments point to the appropriateness and need for the adoption of similar rules in copyright to account for intellectual privacy.

Finally, *CASL* may inform the approach that copyright could take to any ‘opt-out’ requirements in copyright law which permit individuals to opt-out of the collection of their personal information through DRM. While Bill C-11 includes a general opt-out suggestion in section 41.14, *CASL*, rightly or wrongly, includes a much more detailed opt-out (or ‘unsubscribe’) in draft regulations.⁷⁸⁰ For example, it prescribes that individuals must be able to opt out of receiving commercial electronic messages in two clicks. A similar approach could be implemented in respect of opting out of the collection of information by DRM, and in respect of the removal of RMI that diminishes intellectual privacy.

⁷⁷⁹ Jennifer Stoddart, “Making Privacy Protection More Effective for Canadians”, Remarks at the Centre for Law, Technology and Society of the University of Ottawa, January 19, 2011, Ottawa, Ontario, online: Office of the Privacy Commissioner <http://priv.gc.ca/speech/2011/sp-d_20110119_e.cfm>:

We’ve become one of the few major countries where the data protection regulator lacks the ability to issue orders and impose fines. [...]

Here in Canada, the CRTC has the power to impose fines for violations of the do-not-call rules (and recently slapped Bell Canada with a record-setting \$1.3-million penalty). There are significant fines – \$10 million for businesses – provided for in the new anti-spam law.

Hefty fines get just about any company to sit up and take notice – and to place a greater importance on compliance.

⁷⁸⁰ See *supra* note 221.

4. Adopt a modified notice-and-notice regime for ISP liability

If there is to be an ISP liability provision in copyright law at all, in the area of ISP liability and P2P file sharing lawsuits, copyright law could help address privacy implications by (a) requiring that a legal and/or evidentiary threshold be met before a notice could be issued (e.g. that the copyright holder provide a sworn statement in support of their notice, confirming that it has a *prima face* case against the targeted individual(s)), (b) minimizing the time period for the retention of identifying data and (c) requiring ISPs to retain only minimal information – e.g. the name and last known address of the subscriber.⁷⁸¹

The proposal currently included in Bill C-11 (which is based on a voluntary system put in place by some of Canada's largest ISPs) addresses none of the above points, though it is certainly far better (from an intellectual privacy perspective) than a notice-and-takedown regime, or a notice-and-termination regime, which have been considered and implemented in a number of countries outside of Canada.⁷⁸² However, with respect to the length of time for retention, there appears little reason for it to take more than 60-90 days for a plaintiff to take action following the issuance of the notice. The initial six month period set forth in Bill C-11, which can be extended for up to a year when a proceeding is commenced within six months, seems far too long. In addition, the amount of information retained should be the bare minimum needed to identify the person and individuals should be given notice of any

⁷⁸¹ The CBA made the following submission with respect to the notice-and-notice regime proposed in Bill C-32: "The existing de facto "notice and notice" regime in Canada has functioned well for over a decade and should be explicitly sanctioned in the statute. Any extension of the status quo would lead to abuse and intolerable invasions of privacy if it permitted disclosure without a court order." CBA, *supra* note 767 at 5.

⁷⁸² See Chapter 3, Part III.

attempt to bring a claim against them, along with the right to appear through counsel without identifying themselves, *before* any disclosure of identifying information is made. This suggestion is consistent with the question of notice to targeted individuals which has been raised by the courts in recent *Norwich* cases.⁷⁸³

5. Ensure consistency for intellectual privacy in copyright litigation

Finally, to help ensure that intellectual privacy is consistently protected across Canada in the context of P2P and other copyright litigation, copyright law could specifically spell out a privacy-respecting test for courts to apply in determining whether to order ISPs to release subscribers' information in copyright disputes. No such proposals are contained in the current legislative proposals on the table in Canada. While it is certainly arguable that the tests such as those developed in *BMG v Doe* and *Warman v Grosvenor*, provide an appropriate measure of procedural protection for intellectual privacy, the test could benefit from codification in at least two ways.

First, codifying the test in the *Copyright Act* would (in theory) ensure a consistent approach across Canada. Second, since motions to compel third parties (usually ISPs and website operators) to reveal individuals' identity are always or almost always unopposed by the third party and brought without notice to the affected individual, the moving party is often at a distinct advantage in terms of the evidence and argument presented to the court. A codified test could put some parameters around this potential issue (e.g. 'full and frank' disclosure might be required as it is in other *ex parte* motions, an undertaking as to damages might have to be given in the event that the individual is wrongly accused based on the copyright holder's investigation, or certain forms of information regarding the investigation into the alleged infringement might be

⁷⁸³ See e.g. *supra* note 724 and accompanying text.

mandatory in order to minimize the risk that innocent people would be identified). The test could also build in a requirement to give notice to the targeted individual and to permit an appearance through counsel, except where inappropriate.

IV. Conclusions

The foregoing parts of this chapter have endeavoured to complete the case for addressing intellectual privacy within copyright. It has been demonstrated in this chapter why intellectual privacy should not be left to regulatory instruments of general application but instead can and should be addressed within copyright. With reference to the shortcomings of the proposals that have been made to-date in Canada, and drawing on the material discussed in earlier chapters, Part III of this chapter has briefly sketched five basic recommendations for rules that one would expect to see in any copyright law that purported to take intellectual privacy seriously.⁷⁸⁴

⁷⁸⁴ One program of future research to come out of this dissertation is to translate the recommendations provided herein into legislative language.

CONCLUSIONS

It is a commonplace that the characteristic virtue of Englishmen is their power of sustained practical activity, and their characteristic vice 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.⁷⁸⁵

— R.H. Tawney, 1921

Driven by the copyright industries and with the blinkers of those industries in place, DRM 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. Although intellectual privacy and its relationship with copyright have not yet received the attention that they merit, soon, these two marches will certainly collide even more so than they have to date. This dissertation has suggested that we should be very curious about our destination and that we

⁷⁸⁵ RH Tawney, *The Acquisitive Society* (London: G. Bell and Sons, 1921) at 1.

ought to make our own path that accounts for intellectual privacy within copyright.

In particular, this dissertation has made the case for a particular definition of intellectual privacy and, without making empirical claims, has explored whether diminishing it in the name of copyright holders' interests will lead to the impoverishment of the very copyright kingdoms that we purport to be protecting in so doing.

In response to this question, this dissertation has built an argument that individuals' intellectual privacy is an essential component of copyright as a consistent and unified whole and that copyright law can and should explicitly internalize protection of intellectual privacy. Ultimately, this dissertation has formulated principles and five basic recommendations for rules to account for intellectual privacy within the legal concept of copyright.

Had this dissertation included an empirical study of the issues discussed herein, one might have concluded that it is too early to tell what the long-term impact of diminishment of intellectual privacy on the purposes of copyright might be. Most of the examples described in Chapter 1 and 3 are from the past five years and some go back at most about a decade. However, as argued herein, there certainly appear to be good reasons to be concerned. Yet, I am not making predictions.⁷⁸⁶ Instead, I have attempted to address key questions that have come to the fore in light of our present experience, and to craft answers to those questions in an attempt to preserve certain important and fundamental values of intellectual privacy, including for the objectives of copyright.

⁷⁸⁶ Milan Kundera, *Ignorance*, translated by Linda Asher (New York: Perennial, 2002) ("All predictions are wrong, that's one of the few certainties granted to mankind. But though predictions may be wrong, they are right about the people who voice them, not about their future but about their experience of the present moment" at 13).

Given the rapidly evolving technological context in which many of the issues herein play out, this dissertation does not purport to have all of the answers. Copyright and intellectual privacy have only begun to be addressed with the arguments and recommendations for rules proposed above. It is hoped that this dissertation has laid the groundwork to do more work in future, including by building on and implementing in legislation the recommendations proposed herein. Indeed, given that there is an ongoing need to adjust the analysis and rules presented herein, because technologies and business practices change frequently, we will have to return again and again to the important topics and questions raised herein.