SIX

# If Left to Their Own Devices …

## How DRM and Anti-circumvention Laws Can Be Used to Hack Privacy

**Ian R. Kerr***

## A. INTRODUCTION

In the decade since that cold and wet December day — when delegates from 150 countries met to finalize the universal mold for digital copyright reform[1] — billions of keystrokes have been spent, tapping out arguments about whether and to what extent we need new laws to protect the technologies that protect copyright. The prevailing opinion in many countries with strong

* The author wishes to extend his gratitude to the Social Sciences and Humanities Research Council, the Canada Research Chairs program, Bell Canada, and the Ontario Research Network in Electronic Commerce for all of their generous contributions to the funding of the research project from which this paper derives. Special thanks also to Todd Mandel, Shannon Ramdin, Catherine Thompson, and Hilary Young for all of their extraordinary efforts, their brilliance, and for the high quality of research assistance that they so regularly and reliably provide. Thanks also to Jane Bailey, Ann Bartow, Lee Bygrave, Alex Cameron, Julie Cohen, Michael Geist, Daphne Gilbert, Graham Greenleaf, Chris Hoofnagle, Philippa Lawson, David Matheson, Daniel Solove, and Valerie Steeves for the excellent suggestions for improvement that they generously offered.

1 Jessica Litman, "The Bargaining Table" in *Digital Copyright* (Amherst: Prometheus Books, 2001) at 122; Pamela Samuelson, "The U.S. Digital Agenda at WIPO" (1997) 37 Va. J. Int'l L. 369.

copyright industries is that we do.[2] Their most powerful voices[3] tell us that such laws are necessary to protect the copyright industries from individuals who use devices to circumvent the technologies meant to protect copyright. They say that existing laws are not adequate to prevent the massive illegal dissemination of digital works that takes place off and online everyday.[4]

After nearly a decade of indecision, it looks like Canada is finally about to board the Mothership. In its recently released Bill C-60,[5] Canada an-

2 See for example *The Digital Millennium Copyright Act of 1998,* Pub. L. No. 105-304, 112 Stat. 2860, <www.copyright.gov/legislation/dmca.pdf> [*DMCA*]; European Union's *Directive of the European Parliament and the Council of 22 May 2001 on the Harmonization of Certain Aspects of Copyright and Related Rights in the Information Society* (2001), L 167/10, <http://europa.eu.int/information_society/eeurope/2005/all_about/digital_rights_man/doc/directive_copyright_en.pdf> [*EUCD*]; Australia's *Copyright Amendment (Digital Agenda) Act 2000* (Cth.) [Digital Agenda]; *Japanese Copyright Law No. 48*, promulgated on 7 May 1970 as amended by Law No. 77, of 15 June 1999 and the *Japanese Anti-Unfair Competition Law (JAUCL)*; New Zealand's *Copyright Act 1994 No. 143*(N.Z.), as last amended by *Law No. 33, 2005*; and *Copyright Ordinance (Cap. 528)*, entered into force June 1997 (Hong Kong).

3 As the RIAA points out on its website, "RIAA believes that the establishment of technological protection and management of all musical content, regardless of the media on which it resides or the method by which it is transmitted, is a central component for the expansion of both the music opportunities for the consumer and the business opportunities for the consumer and the business opportunities for the technology industry," <www.riaa.com/issues/audio/newmedia.asp> at "Protecting Rights on Networks"; CRIA states in its submission to the Canadian Copyright Reform Process "Law and technology must be used together to maintain adequate incentives for creativity. Failure to offer adequate legal protection to technological protection measures (TPMs) will inevitably inhibit the development of electronic commerce in copyrighted products," <http://strategis.ic.gc.ca/epic/internet/incrp-prda.nsf/en/rp00249e.html>.

4 I and others remain unconvinced and have argued elsewhere against this position: Ian R. Kerr, Alana Maurushat, & Christian S. Tacit, "Technological Protection Measures: Part I — Trends in Technical Protection Measures and Circumvention Technologies" (2003) commissioned by the Department of Canadian Heritage (Canada), <www.pch.gc.ca/progs/ac-ca/progs/pda-cpb/pubs/protection/tdm_e.cfm>; Ian R. Kerr, Alana Maurushat, & Christian S. Tacit, "Technological Protection Measures: Part II – The Legal Protection of TPMs" (2003) commissioned by the Department of Canadian Heritage (Canada), <www.pch.gc.ca/progs/ac-ca/progs/pda-cpb/pubs/protectionII/tdm_e.cfm>; Ian R. Kerr, Alana Maurushat, & Christian S. Tacit, "Technical Protection Measures: Tilting at Copyright's Windmill" (2003) 34:7 Ottawa L. Rev. 82 [Kerr *et al*., "Tilting at Copyright's Windmill"].

5 Bill C-60, *An Act to amend the Copyright Act,* 1st Sess., 38th Parl., 2005, Preamble [*Copyright Amendment*], <www.parl.gc.ca/PDF/38/1/parlbus/chambus/house/bills/government/C-60_1.PDF>.

nounced that it will implement the *WIPO Copyright Treaty*[6] and the *WIPO Performances and Phonograms Treaty*[7] by tabling its own anti-circumvention laws. The core provision will entitle a copyright owner to copyright and common law remedies against anyone who, without the consent of the copyright owner, "circumvents, removes, or in any way renders ineffective a technological measure protecting any material form of the work ... for the purpose of an act that is an *infringement of the copyright* in it or the moral rights in respect of it or for the purpose of making a copy referred to in subsection 80(1)."[8] A second provision will generate a similar result for anyone who "knowingly removes or alters any rights management information in electronic form ...."[9]

In essence, these *paracopyright* provisions are meant to add a new legal layer, one that goes beyond existing copyright and contract laws in order to deter and provide legal remedies against individuals who, for "infringing purposes," hack past content-protecting technologies[10] that automatically enforce access to or uses of digital material. A central aim of the proposed legislation[11] is "to provide rights holders with greater confidence to exploit the Internet as a medium for the dissemination of their material and provide consumers with a greater choice of legitimate material."[12] These are certainly laudable goals. However, it remains uncertain whether Canada's proposed anti-circumvention provisions will in fact do less

---

6 *WIPO Copyright Treaty*, 20 December 1996, 36 I.L.M. 65 (entered into force 2 March 2002) [*WCT*], <www.wipo.int/treaties/en/ip/wct/trtdocs_wo033.html>.

7 *WIPO Performances and Phonograms Treaty,* 20 December 1996, 36 I.L.M. 76 (entered into force 20 May 2002) [*WPPT*], <www.wipo.int/treaties/en/ip/wppt/trtdocs_wo034.html>.

8 *Copyright Amendment,* above note 5, s. 34.02 (emphasis added).

9 *Ibid*., s. 34.01.

10 Graham Greenleaf distinguishes "content-protecting" from "copyright-protecting" technologies because the former "protect content which copyright does not protect." 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"] at 14. In order to remain consistent with the language used in the proposed legislation, in this chapter I will refer to all such technologies as TPMs.

11 *Copyright Amendment,* above note 5.

12 *Statement — Government Statement on Proposals for Copyright Reform*, March 2005, [*Statement*], <http://pch.gc.ca/progs/ac-ca/progs/pda-cpb/reform/statement_e.cfm>.

harm to copyright's delicate balance[13] than the laws enacted in the United States,[14] Europe,[15] and elsewhere.[16]

What is less uncertain is the effect of the proposed anti-circumvention law on personal privacy. When it comes to protecting intellectual privacy[17] — a core value underlying the doctrine of intellectual property — the recently released Bill C-60[18] 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 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. The best solution from a privacy perspective is no legal protection for TPMs at all. However, if the copyright industries and the government insist on claiming a legitimate need for new laws to prevent the circumvention of TPMs, then similar provisions are needed to protect citizens from organizations that use both TPMs and the law of contract as a kind of privacy circumvention device. Copyright owners should not be encouraged or allowed to

---

13 *CIPPIC Questions Unbalanced Copyright Bill,* 20 June 2005, <www.cippic.ca/en/news/documents/Media_Release_-_Copyright_Bill_-_20_June_05_Final.pdf>.

14 17 U.S.C. § 1201(a)(1)(A) (2001).

15 *EUCD*, above note 2 at 17 (Article 6(1), 6(2), 7(1)).

16 Australia: *Copyright Act 1968* (Cth.), Act No. 63 of 1968 as amended, 2005, s. 116A <www.comlaw.gov.au/ComLaw/Legislation/ActCompilation1.nsf/framelodgmentattachments/DBD28FED04130B18CA256FE7008378BB>; Japan: *Japanese Copyright Law No. 48* promulgated on 7 May 1970, as amended by Law No. 92, of 9 June 2004, Article 30(1) <www.cric.or.jp/cric_e/clj/clj.html>; Hong Kong: *Copyright Ordinance* (Cap 528, 1997, H.K.), s. 273-4; New Zealand: *Copyright Act 1994* (N.Z.), 1994/143, as amended by Law No.33 2005, s. 226 <www.legislation.govt.nz/browse_vw.asp?content-set=pal_statutes>.

17 That is, the right to experience intellectual works in private, free from surveillance. See, for example, Julie Cohen, "A Right to Read Anonymously: A Closer Look at 'Copyright Management' in Cyberspace" (1996) 28 Conn. L. Rev. 981 at 1003 [Cohen, "A Right to Read Anonymously"]; Julie Cohen, "DRM and Privacy" (2003) 18 Berkeley Tech. L.J. 575 at 584 [Cohen, "DRM and Privacy"]; Greenleaf, above note 10 at 16.

18 *Copyright Amendment*, above note 5.

use TPMs and contracts to circumvent fair information principles[19] or to hack past data protection legislation. In this brief chapter, I will explain why this is so and will offer a general description of the kind of countermeasures that are needed.

## B. DIGITAL RIGHTS MANAGEMENT

In choosing to implement the *WCT* and *WPPT*, the Government of Canada has adopted the position that the legal protection of TPMs is necessary. In order to better grasp the social ramifications of adopting this position, it is crucial to understand the role that TPMs play within a grander system of intertwining technologies and legal mechanisms that are being used to establish a secure global distribution channel for digital content.

As I and others have suggested elsewhere,[20] it is useful to distinguish between TPMs and the digital rights management (DRM) systems in which they often play a role. In its simplest form, a TPM is a technological measure intended to promote the authorized use of digital works. This is accomplished by controlling access to such works, or various uses of such works, including: (i) copying, (ii) distribution, (iii) performance, and iv) display.[21] To illustrate, Sony has developed a technological measure that allows owners of its PlayStation console to play only authorized copies of Sony's games (e.g., only versions that are sold for use in the same geographic region where the game console is bought).[22] As Charles Clark famously put it, Sony thought that "the answer to the machine is in the machine."[23]

Although the TPM plays a role in promoting authorized uses of Sony's PlayStation, one must remember that, in a hacker's world, the *answer* to

---

19 Organisation of Economic Co-operation and Development, *Guidelines on the Protection of Privacy and Transborder Flows of Personal Data* (Paris: OECD Publications, 1980), <www.oecd.org/document/18/0,2340,en_2649_34255_1815186_1_1_1_1,00.html> ["OECD Guidelines"]; Canadian Standards Association, *Model Code for the Protection of Personal Information* (CSA Publications, 1996), <www.csa.ca/standards/privacy/code/Default.asp?language=English>; *Personal Information Protection and Electronic Documents Act,* S.C. 2000, c. 5, Schedule 1, <www.privcom.gc.ca/legislation/02_06_01_01_e.asp> [*PIPEDA*].

20 Kerr *et al*., above note 4 at 26.

21 Mark Perry & Casey Chisick, "Copyright and Anti-circumvention: Growing Pains in a Digital Millennium" (2000) New Zealand Int. Prop. J. 261.

22 *Stevens v. Kabushiki Kaisha Sony Computer Entertainment & Ors* [2005] HCA Trans 30 (8 February, 2005 (High Court of Australia) [*Stevens v. Sony*].

23 Charles Clark, "The Answer to the Machine is in the Machine" in Bernt Hugenholtz, ed., *The Future of Copyright in a Digital Environment: Proceedings of the Royal Academy Colloqium* (1996) at 139.

the answer-in-the-machine is *also* in the machine. That is, other technologies can be used to circumvent the Sony TPM. "Mod chips," as they became known, have been used to do just that, causing Sony to seek and obtain special leave to appeal to the Australian High Court for its interpretation of the anti-circumvention provisions in the *Copyright Amendment (Digital Agenda) Act*.[24]

It is noteworthy that TPMs can operate as a kind of "virtual fence"[25] around digitized content and can therefore be used to lock-up content — whether or not it enjoys copyright protection. A TPM can be used on its own, or as a building block in a larger system of technological and legal mechanisms, often referred to as DRM.

DRM is a generic term describing a set of technologies that can identify content and set out licensing conditions. More and more, DRMs rely on TPMs to manage the rights that coincide with digital content.[26] Typically, a DRM consists of two components. The *first component* is a set of technologies that might include: "encryption, copy control, digital watermarking, finger-

24 *Digital Agenda*, above note 2; *Stevens v. Sony*, above note 22. In the *Stevens* case, the Australian High Court was called upon to determine whether Sony's "access code" embodied on each track of each Playstation CD-ROM, when used in conjunction with a "boot ROM" chip located on the circuit board of the console, falls within the legal definition of "technological protection measures" pursuant to s. 10(1) of the Act. Although this case raises various policy considerations regarding the appropriate interpretation of s. 10, it also illustrates that not all copy protection technologies will be protected by anti-circumvention laws. For an excellent discussion of the High Court's analysis and further insight into the policy implications of this case (both before and after the Australia-United States Free Trade Agreement), see Kimberlee Weatherall, "On Technology Locks and the Proper Scope of Digital Copyright Laws – Sony in the High Court" (2004) Syd. L. Rev. 41.

25 Authors including Ejan Mackaay have used the metaphor of the digital fence to illustrate how intangible property may be protected. Fencing techniques such as TPMs or contractual arrangements allow rightsholders the ability to control access to and, in some circumstances, the use of their works. Such metaphors build on the notion articulated by Robert Ellickson who discussed how the invention of barbed wire allowed smaller lots to be used for breeding cattle, thereby changing the economics of such land use. See Ejan MacKaay, "Intellectual Property and the Internet: The Share of Sharing," in Neil Netanel, Niva Elkin-Koren, & Victor Bouganim, eds, *The Commodification of Information* (The Hague: Kluwer Law International, 2001). See also Robert Ellickson, "Property in Land" (1993) 102 Y. L. J. 1315.

26 Mark Stefik, "Shifting the Possible: How Trusted Systems and Digital Property Rights Challenge us to Rethink Digital Publishing" (1997) 12 Berkely Tech. L.J. 137 cited in Canada, Canadian Heritage, <www.pch.gc.ca/progs/ac-ca/progs/pda-cpb/pubs/protection/2_e.cfm?nav=0>.

printing, traitor tracing, authentication, integrity checking, access control, tamper-resistant hard and software, key management and revocation as well as risk management architectures."[27] Some of these technologies are used to *enforce* corporate copyright policies and pricing schemes imposed by a DRM through a registration process that requires purchasers to hand over certain bits of personal information. As Lee Bygrave describes it:

> The registration could be stored centrally within the system and/or embedded as (part of) digital watermarks in the works themselves. The works might also be configured to enable ongoing (or periodical) registration of the way in which they are used by the purchaser, transmission of these usage data back to a central monitoring service provider, and/or automatic renewal/modification of usage rights on the basis of online interaction with the provider — i.e., what Greenleaf aptly terms *"IP phone home."* [28]

In addition to its ability to "phone home," other technologies are used to *express* copyright permissions in "rights expression languages" and other forms of metadata that make a DRM policy machine-readable.[29] Rights expression languages are the bridge to the *second component* of DRM, which consists of a set of legal permissions. In the current context, these permissions are typically expressed as a licensing arrangement which, by way of contract, establish the terms of use for the underlying work.[30]

---

27 Stefan Bechtold, "The Present and Future of Digital Rights Managements – Musings on Emerging Legal Problems" in Eberhard Becker et al., eds. *Digital Rights Management* (Berlin: Springer Verlag, 2003), 597 at 598 [Bechtold, "The Present and Future of Digital Rights Management"], <www.jura.uni-tuebingen.de/bechtold/pub/2003/Future_DRM.pdf>.

28 Lee A. Bygrave, "Digital Rights Management and Privacy — Legal Aspects in the European Union" in Eberhard Beckar *et al*., eds. *Digital Rights Management — Technological, Economic, Legal and Political Aspects* (New York: Springer, 2003) 418 at 421 [Bygrave, "Digital Rights Management and Privacy"].

29 Bechtold, above note 27 at 598–99.

30 Hugenholtz has defined DRM as a contract, typically a licensing agreement, coupled with technology, typically a technological protection measure such as encryption: 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) The Journal of Electronic Publishing, <www.press.umich.edu/jep/04-03/gervais.html>. Given that DRM can be used to manage permissions beyond copyright, the second component need not look anything like typical IP licenses. As Jonathan Weinberg has put it, "[t]he term 'rights management' is commonly associated with the protection of intellectual property rights, but

The technological components of most full-blown DRMs are linked to a database which enables the automated collection and exchange of various kinds of information among rights owners and distributors about the particular people who use their products; their identities, their habits, and their particular uses of the digital material subject to copyright.[31] The information that is collected and then stored in these databases can be employed in a number of different ways. For example, it could be employed to promote the authorized use of an e-book by restricting access only to those who have paid to use the work, or by restricting their ability to subsequently distribute it to others who have not. Other related applications of the database usage information include the ability to identify the user's machine in order to prevent use of the material on other machines or to restrict the total number of times that the work can be accessed by that machine.

The surveillance features associated with the database are crucial to the technological ment of the licensing component. It is through the collection and storage of usage information that DRMs are able to "authorize use" in accordance with the terms of the licensing agreement and thereby "manage" copyrights.[32]

Together, the database and the license allow owners of digital content to unbundle their copyrights into discrete and custom-made products. And, since they are capable of controlling, monitoring, and metering most uses of a digital work, DRMs can be linked to royalty tracking and accounting systems. On this basis, DRM optimists believe that it will offer a secure framework for distributing digital content, promising that copyright owners will receive adequate remuneration while enabling a safe electronic marketplace that offers to consumers previously unimaginable

---

it need not be so limited. One can think of rights management as covering any technological means of controlling public access to, and manipulation of, digital resources. That sort of control is basic to any system of networked computing." See Jonathan Weinberg, "Hardware-Based ID, Rights Management, and Trusted Systems" (2000) 52 Stan. L. Rev. 1251 T 1255, <http://cyber.law.harvard.edu/ilaw/Contract/Weinberg_Full.html>, [Weinberg, "Hardware-Based ID"].

31 Ian R. Kerr & Jane Bailey, "The Implications of Digital Rights Management for Privacy and Freedom of Expression" (2004) 2 Info. Comm. & Ethics in Society 87 [Kerr & Bailey, "Implications of Digital Rights Management"].

32 Jeffrey P. Cunard, "Technological Protection of Copyrighted Works and Copyrighted Management Systems: A Brief Survey of the Landscape," ALAI Congress 2001, at 2 [Cunard, "Technological Protection"] <www.alai-usa.org/2001_conference/pres_cunard.doc>.

business models beyond sales and subscriptions, such as highly individualized licensing schemes with variable terms and conditions.[33]

## C. DIGITAL ROUTINE MONITORING?

While much of the above sounds extremely promising for copyright holders and even for consumers who want alternatives to traditional music album formats, etc., there is a dark side to DRM's monitoring and metering capabilities. From this perspective, DRM's glass is half empty. DRM has the ability to monitor an individual's private activities while browsing, sampling, or shopping.[34] But it can also be used to collect information or monitor behaviour after a contract is entered into, with the aim of checking compliance with the contract. While it may be linked to the notion of contractual performance, DRM has the ability to "capture in its net a range of personal data that are not strictly required for compliance purposes."[35] As Greenleaf has so colorfully characterized it, "IP can phone home to check that it should still be at your place, and there are very considerable limits to what you and others can do about it."[36]

---

33 For example, DRMs also make it possible to offer site licences based on numbers of simultaneous users or linked to specific hardware. Terms of use can be based on limited and unlimited use, or time-related use. See, for example Carol Risher, "Technological Protection Measures (Anti-Circumvention Devices) and their Relation to Exceptions to Copyright in the Electronic Environment" (Paper presented to the *IPA Copyright Forum, Frankfurt Book Fair*, 20 October 2000) at 5.

34 See, generally, Lee A. Bygrave, "The Technologisation of Copyright: Implications for Privacy and Related Interests" (2002) European Intellectual Property Review, vol. 24(2) 51 [Bygrave, "The Technologisation of Copyright"].

35 Bygrave above note 28 at 432. See generally, *ibid*.

36 Greenleaf, above note 10 at 53. For example, in 1999 the maker of the popular "RealJukebox" software, embedded a "Globally Unique Identifier" (GUID) that was capable of combining music-listening habits with personal information such as home addresses and credit card numbers. Only after public outcry did they pull this version of their player from the market: Courtney Macavinta, "RealNetworks puts a patch on privacy concerns," *CNET News.com* (1 November 1999), <http://news.com.com/2100-1040-232268.html?legacy=cnet>. Although most popular commercial music sites have learned from the RealJukebox experience, placing limits on the disclosure to third parties of personal information linked with usage statistics, services such as "Napster to Go" collect personal usage information, including "... tracks that you may have listened to offline on compatible portable devices," and "... use your personally identifying usage data for a variety of service-related purposes," Napster Privacy Policy, <www.napster.com/privacypolicy.html> (29 January 2005).

It should therefore be evident that a full-blown DRM is much more than just a "virtual lock" or "digital fence." Alex Cameron recently described them as follows:

> 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.[37]

Surprisingly, the bulk of writing on the subject of DRM has, to date, focused primarily on copyright policy. Despite the fact that the capacity to monitor and meter customer habits is an essential feature of DRM, the level of sustained focus on the privacy aspects of DRM in Canada is practically nil[38] and, worldwide, is surprisingly sparse.[39] As Julie Cohen has noted:

---

37 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 19th International Information Security Workshops, 22–27 August 2004, (Toulouse, France: Kluwer, 2004) at 2, <www.anonequity.org/bigfiles/Alex%20Cameron%20-%20Infusing%20Privacy%20Norms%20in%20DRM.pdf> [Cameron, "Infusing Privacy Norms in DRM"].

38 Ontario's Information and Privacy Commissioner wrote an excellent article uncovering the issues in 2002: Ann Cavoukian, "Privacy and Digital Rights Management (DRM): An Oxymoron?" (2002) Information and Privacy Commissioner/Ontario, <www.ipc.on.ca/docs/drm.pdf>; Kerr & Bailey, above note 31; A. Cameron, "Digital Rights Management: Where Copyright and Privacy Collide" (2004) 2 C.P.L.R. 14 [Cameron, "Digital Rights Management"]; Geist, "Canada Rejects One-Sided Approach to Copyright Reform" *The Toronto Star,* (28 March 2005); <www.michaelgeist.ca/resc/html_bkup/mar282005.html>, Michael Geist, "'TPMs': A perfect storm for consumers" *The Toronto Star* (31 Jan 2005) <www.michaelgeist.ca/resc/html_bkup/jan312005.html>; Michael Geist, "Canada's on-line copyright policy takes shape" *The Globe and Mail* (12 July 2001), <http://news.globetechnology.com/servlet/GAMArticleHTMLTemplate?tf=globetechnology/TGAM/NewsFullStory.html&cf=globetechnology/tech-config-neutral&slug=TWGEISY&date=20010712>.

39 Bechtold, above note 27; Lee A. Bygrave & Kamiel Koelman, "Privacy, Data Protection and Copyright" in Bernt Hugenholtz, ed., *Copyright and Electronic Commerce: Legal Aspects of Electronic Copyright Management* (The Hague: Kluwer Law International, 2000); Bygrave, "The Technologisation of Copyright," above note 34; Bygrave, "Digital Rights Management and Privacy," above note 27; Cohen, "A Right to Read Anonymously," above note 17; Cohen, "DRM and Privacy," above note 17; Michael Einhorn, "Digital Rights Management, Licensing, and Privacy" (2002), <http://papers.ssrn.com/sol3/papers.cfm?abstract_id=332720>; Greenleaf, "IP, Phone Home," above note 10; Weinberg, "Hardware-Based ID," above note 30.

> For the most part, the privacy implications of DRM systems go unexamined in the mainstream legislative and policy debates about the proper scope of a copyright owner's rights. Instead, courts and some commentators (and many intellectual property lawyers) have challenged the design of DRM systems as grounded, unproblematically, in principles of copyright and justified by reference to a copyright owner's need to enforce its "property rights." Yet it is far from obvious why this should be so.[40]

Graham Greenleaf — one of a handful of other scholars who have published extensively on this subject — shares Cohen's concern. According to Greenleaf, "[i]n the worst scenarios, the surveillance mechanisms being developed ... may ... bring about the end of the anonymity of reading."[41]

It is worth noting that the paucity of policy debate around the privacy issues is not because these issues arose recently or unexpectedly. In fact, Cohen presciently diagnosed the problem the very same year that *WCT* and *WPPT* were carved into silicon:

> 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. The same technologies that have made vast amounts of information accessible in digital form are enabling information providers to amass an unprecedented wealth of data about who their customers are and what they like to read. In the new age of digitally transmitted information, the simple, formerly anonymous acts of reading, listening, and viewing — scanning an advertisement or 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.[42]

Although referred to as "rights management" systems, what DRM *really* manages is people — by collecting information about them 24/7 through automated, often surreptitious surveillance technologies.[43]

---

40 Julie Cohen, "Overcoming Property: Does Copyright Trump Privacy?" (2002) U. Ill. J.L. Tech & Pol'y 375 [Cohen, "Overcoming Property"], <www.law.georgetown.edu/faculty/jec/overcomingproperty.pdf>, at 102.

41 Greenleaf, above note 10 at 14.

42 Cohen, "A Right to Read Anonymously," above note 17 at 981.

43 See generally, Kerr & Bailey, "Implications of Digital Rights Management," above note 31 at 89.

Through the collection of information, DRM affects a shift in social power by exacting greater control over information and, more crucially, knowledge. DRM entails a disenfranchisement through the erosion of previously enjoyed public spaces in which knowledge was shared and transferred outside the eye of the powerful — in other words, privately. DRM is a technology of the powerful, for the powerful, that seeks to invade previously private spaces and reconstruct and control individual actions for its own purposes. The erosion of privacy goes beyond the individual, and as the space for private, autonomous action shrinks, there are significant political consequences. From this perspective, DRM is a form of social control.[44]

Since the purpose of the proposed anti-circumvention provisions is to enable DRM and to facilitate its implementation as a primary means of enforcing digital copyright, it should not be difficult to see that privacy protection becomes an increasingly significant consideration in contemplating the details of Canada's proposed anti-circumvention provisions. After all, DRM and other technologies adopted by the private sector displace the adage that one's home is one's castle. The moats are long gone, and it is no longer sufficient to draw the blinds. DRM enables — and the law in many jurisdictions currently permits — surveillance within what was once the seclusion of our homes, including "the ability to collect fine-grained information about uses of DRM-protected content and the ability to reach into [citizens'] homes and restrict what they can do with copies of works for which they have paid."[45] With an increasing reliance on automation and wireless technologies, these monitoring systems are becoming our more constant companions, wherever we go. The key difference is that these companions are seeking to monitor what is going on in *our heads*. This is a dangerous practice to allow, especially when one considers that many of the corporations building these mechanisms of social control into the content delivery system are also attempting to corner the production market as well, embedding corporate imperatives into the content itself right across the spectrum. When this happens, the erosion of public spaces for debate and thoughtful exchange disappear because the roadway *and* the scenery are artificially controlled.[46]

---

44 I owe this point to Valerie Steeves.

45 Cohen, "Overcoming Property," above note 40, 41 at 101.

46 I owe this point to Valerie Steeves.

## D. PRIVACY'S PLACE IN THE "APPROPRIATE BALANCE"

Copyright policy, freedom of expression, and access to information issues aside,[47] it should be evident from the above description that the current, mainstream orientation of DRM could have the effect of shifting certain public powers into the invisible hands of private control. Given DRM's extraordinary surveillance capabilities, it is extremely difficult to imagine why the Government of Canada has failed to address *any* aspects of the privacy implications of DRM in drafting its anti-circumvention provisions. Especially, in light of legislative reforms that use the law to further enable DRM and to facilitate its implementation as a primary means of enforcing digital copyright. In this new role, DRM will be ambient, ubiquitous, and omnipresent.

Clearly, the mere existence of Canada's federal data protection legislation is not the reason.[48] The more likely explanation is the increasingly common misconception, recently exemplified by the Federal Court of Appeal, that, "[a]lthough privacy concerns must ... be considered ... they must yield to public concerns for the protection of intellectual property rights in situations where infringement threatens to erode those rights."[49] Although this point of view has gained much currency in a world where powerful property stakeholders and private sector lobbyists are often able to set the agenda, this perspective is problematic. Intellectual property rights are in-

47 These subjects are dealt with elsewhere in this book in chapters 1, 9, & 19.

48 With more bark than bite, *PIPEDA* codifies an abstract set of fair information principles, but 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: *PIPEDA,* above note 19, s. 12. Likewise, the Privacy Commissioner has no power to order damages. That remedy is limited to the courts: *PIPEDA,* above note 19 s. 16(c). Further, the administrative process requires that the complaint be brought to the Privacy Commissioner first, creating cost burdens for the complainant and significant delays in the ultimate resolution of conflicts by the courts. See Generally, Michael Geist, "Weak enforcement undermines privacy laws" *The Toronto Star* (19 April 2004) <www.michaelgeist.ca/resc/html_bkup/april192004.html>.

49 *BMG Canada Inc. v. John Doe*, 2005 FCA 193, [2005] F.C.J. No. 858, <www.fca-caf.gc.ca/bulletins/whatsnew/A-203-04.pdf>, Sexton J. at para. 41. But see Lebel J. *Society of Composers, Authors and Music Publishers of Canada v. Canadian Assn. of Internet Providers*, [2004] 2 S.C.R. 427, <www.canlii.org/ca/cas/scc/2004/2004scc45.html>, at para. 153 who says that: "Insofar as is possible, this Court should adopt an interpretation ... that respects end users' privacy interests, and should eschew an interpretation that would encourage the monitoring or collection of personal data gleaned from Internet-related activity within the home."

deed a fundamental component in the "appropriate balance" contemplated by the *Copyright Act*[50] and the courts' interpretation of it.[51] Still, the "property" rationale and the Government's goal of "provid[ing] rights holders with greater confidence to exploit the Internet as a medium for the dissemination of their material and … consumers with a greater choice of legitimate material,"[52] are an insufficient basis for permitting DRM to circumvent privacy whenever there is a conflict.[53] The presumption that property must trump privacy, or even that it generally trumps, is "far too narrow, and ignores a number of important public policy considerations."[54]

Although it is beyond the scope of this chapter to attempt a survey of all relevant public policy considerations[55] in determining an "appropriate

50 *Statement,* above note 12.

51 See for example, *Theberge v. Galerie d'Art du Petit Champlain Inc. et al* (2002), 210 D.L.R. (4th) 385 (S.C.C.), 285 N.R. 267, Binnie J. at para. 30: "The *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 …. 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 interpreting the *Copyright Act*, courts should strive to maintain an *appropriate balance* between these two goals." (Emphasis added).

52 *Statement,* above note 12.

53 Whether to enable the piracy of personal information or generally to monitor citizens' behaviour.

54 Cohen, "Overcoming Property" above note 40 at 102. Built into this presumption is a failure to recognize the appropriate limits to intellectual property, which, I shall argue below, is itself the result of a failure to recognize appropriate limits of DRM licences.

55 A fourth public policy consideration not fully addressed here is the privacy protection afforded by the *Canadian Charter of Rights and Freedoms*. The *Charter* is relevant in two ways. First, it protects and places a high value on privacy. Second, although private actors do not attract *Charter* scrutiny, it is plausible that the *Charter* is operative in circumstances where private DRM surveillance is enabled by Government-enacted laws.

On the first point, the courts have equated protection from unreasonable search and seizure with a reasonable expectation of privacy and have interpreted that expectation broadly: *Hunter v. Southam Inc.*, [1984] 2. S.C.R. 145 at 159–60. Courts have adopted a purposive approach, noting that privacy: (i) is grounded in physical and moral autonomy, (ii) is essential for the well-being of the individual, and (iii) goes to the essence of a democratic state: *R. v. Dyment* [1988] 2 S.C.R. 417 at 17.

On the second point, it is unclear whether the privacy guarantees set out in the *Charter* are applicable in the case of DRM. Section 32(1) states that the *Charter* applies only to government. The Supreme Court of Canada has made some attempts to define what constitutes governmental action for the purposes

balance" for DRM and privacy, in this section, I will briefly consider three: (i) the Anonymity Principle; (ii) Individual Access; and (iii) DRM Licenses. These will form the basis for three recommendations that I will then offer in response to Canada's proposed anti-circumvention laws in the section that follows.

### 1) The Anonymity Principle

The ability to disconnect one's identity from one's actions is of tremendous instrumental value to intellectual development and intellectual achievement. Millions of people use the Internet to experiment, engaging in a social process of self-discovery by testing the plasticity of their identities and the social norms from which they are constituted.[56] The ability to use "nyms" — alternative identifiers that can encourage social experimentation and role playing — is "an important part of the rich fabric of human culture."[57]

More generally, the ability to be anonymous has significant social utility, facilitating the flow of information and communication on public issues,

---

of s. 32(1), holding that some government intervention (such as delegating legislative powers) would be required for the *Charter* to apply to private parties: *Retail, Wholesale and Department Store Union, Local 580 v. Dolphin Delivery*, [1986] 2 S.C.R. 573 at para. 39.

In the case of DRM, the Government's choice to develop a legislative regime that protects and even promotes DRM surveillance (by prohibiting circumvention) could in some circumstances have the effect of delegating law-making power to private parties. This is achieved by enabling the stronger party to decree and then automate the enforcement of private rules in a manner that interferes with individuals' ability to exercise privacy rights or (re)claim their reasonable expectation of privacy. Although DRM surveillance is itself a private activity, the enactment of anti-circumvention legislation designed to protect DRM's surveillance capabilities might in this sense be said to constitute governmental action of the sort capable of attracting *Charter* scrutiny. Alternatively, even if the *Charter* is itself inapplicable, the values it represents may well be relevant, as the Supreme Courts has held that: "the judiciary ought to apply and develop the principles of the common law in a manner consistent with the fundamental values enshrined in the Constitution.": *Dolphin Delivery* at para. 39.

Although further development of a constitutional argument is beyond the scope of this chapter, suffice it to say that constitutional issues are not irrelevant to a discussion of DRM and privacy.

56 Ian R. Kerr & Alex Cameron, "Nymity, P2P & ISPs" in *Privacy and Identity: The Promise and Perils of a Technological Age* (Kluwer Academic Publishing) [forthcoming 2005].

57 Roger Clark, *Famous Nyms* (31 August 2004), <www.anu.edu.au/people/Roger.Clarke/DV/FamousNyms.html>.

safeguarding personal reputation and lending voice to individual speakers who might otherwise be silenced by fear of retribution.[58] Anonymity can enhance privacy by making it more difficult for others to control the collection, use, and disclosure of one's personal information. Anonymity can also be used to protect people from unnecessary or unwanted intrusions and to "encourage attention to the content of a message or behavior rather than to the nominal characteristics of the messenger."[59] Intellectual consumption and exploration often require a similar sort of social disconnect.[60] Privacy's goal of becoming "more or less inaccessible to others, either on the spatial, psychological or informational plane,"[61] is often an important part of the process of intellectual achievement.

Like intellectual property, the social utility of anonymity has limits. As Lawrence Lessig once remarked, in its broader context, "[p]erfect anonymity makes perfect crime possible."[62] While illegal copying of MP3s is unlikely to unravel civilization as we know it, a more generalized ability to commit perfect crime might. There are good reasons to fear a society in which people believe that they are able to act with impunity. Perfect anonymity would enable those who wish to engage in wrongdoing to step outside of existing social norms by undermining the usual mechanisms of accountability and making it extremely difficult for law enforcement agencies to apprehend them. Fortunately, as Jonathan Weinberg astutely points out, the Internet presents an imperfect blend of anonymity and identifiability; a space where the prospect of true anonymity is often more apparent than real.[63]

But, as the previous section illustrated, that blend of anonymity and identifiability could substantially change with DRM thrown into the mix.

---

58 See generally, Gary T. Marx, "What's in a Name? Some Reflections on the Sociology of Anonymity" (1998) 15(2) Info. Soc'y 99; A. Michael Froomkin, "Anonymity in the Balance" in Chris Nicoll et al. eds., *Digital Anonymity and the Law* (Cambridge: Cambridge University Press, 2003).

59 Marx, *ibid*.

60 Cohen, "DRM and Privacy," above note 17 at 576.

61 Bygrave, "Digital Rights Management and Privacy," above note 28 at 420. See also Ruth Gavison, "Privacy and the Limits of Law" (1980) 89 Yale L.J. 421 at 422. It is for this reason that many jurisdictions have adopted legal measures to limit what might be known about what an individual borrows from a library, rents from a video store, or subscribes to from a cable network.

62 Lawrence Lessig, "The Path of Cyberlaw" (1995) 104 Yale L.J. 1743 at 1750. See also A. Michael Froomkin, *Anonymity and Its Enmities* (June 1995) J. Online L. Art. 4, <www.wm.edu/law/publications/jol/95_96/froomkin.html>, at para. 46.

63 Weinberg, "Hardware-Based ID, Rights Management, and Trusted Systems," above note 30 at 1259.

Recall that "IP phone home" and other features of DRM can be used to reduce or eliminate an individual's ability to consume intellectual goods anonymously. In analog environments, we can buy books, CDs, movies and the like by paying with cash. Paperbacks cannot report back to publishers about their usage.[64] By imposing a network of automated transactions between distributors, their products, users, and use, DRM threatens intellectual achievement by reducing the privacy in intellectual pursuits.

It is crucial to mention that DRM need not impose such threats. To say that DRM is inherently privacy-invasive is to commit what Lessig once referred to as the *IS-ism*.[65] Paraphrasing Lessig, to commit this fallacy is to confuse how something is with how it must necessarily be. While the preceding section attempted to characterize DRM as it is, there is no reason why DRM has to remain this way rather becoming something else. There is in fact

> ... an emerging scholarship which asks how DRM systems could be altered in a value-centered design process so that important policy and legal values are preserved.[66]

Many of the writers in this field recognize that respecting end-user privacy in fact makes good business sense. To commence such a project, though, one must first articulate the purpose of DRM. Weinberg very thoughtfully distilled its *raison d'être* as follows:

> [...] content providers wish to be sure that a packet stream requesting access comes from a person who has paid or is otherwise entitled to access.[67]

---

64 Greenleaf, above note 10 at 17.

65 Lawrence Lessig, *Code and Other Laws of Cyberspace* (New York: Basic Books, 1999) at 24–29 [Lessig, "Code and Other Laws"].

66 Bechtold, above note 27 at 599. See also Stefan Bechtold, "Value-Centered Design of Digital Rights Management – Perspectives on Emerging Scholarship" (2004), INDICARE Monitor Vol. 1, No. 4, <www.indicare.org/tiki-read_article.php?articleId=39>; Cohen, "DRM and Privacy," above note 17; Cameron, "Infusing Privacy Norms in DRM," above note 37; Batya Friedman, Peter H. Kahn Jr., & Alan Borning, "Value Sensitive Design and Information Systems" in Ping Zhang & Dennis Galletta, eds., *Human-Computer Interaction in Management Information Systems: Foundations* (New York: M.E. Sharpe, Inc., 2004); Helen Nissenbaum, "Values in Design," <www.nyu.edu/projects/valuesindesign/index.html>.

67 Weinberg, above note 30 at 1279. For present purposes, I will fully ignore the burning policy issues around whether DRM should be allowed to create a *de facto* access-control right, which I have addressed elsewhere, see Kerr et al.,

Weinberg goes on to say that achieving this end *does not* require pervasive monitoring, nor does it require the collection of personal information about identifiable individuals. The only design feature that the content provider really needs is a means of verifying that the person seeking access or use has the right credentials; that is, that the person has sufficient money or credit, that he is old enough to view the content, that she resides in the jurisdiction making her eligible to vote, etcetera.[68] Interestingly, this idea is not a new one. In fact, as Weinberg notes, David Chaum addressed these issues two decades ago and provided proofs for how it could be achieved. In short, the methods of cryptography — a key technology of DRM — can be used to prove one's credentials without any need to demand or log that person's identity.[69] The method allows content owners to enforce contractual restrictions and hold users accountable without the need to collect personal information, monitor, or meter their behaviour. To the extent that this is possible and DRM continues to collect, monitor, and meter behaviour, DRM is an express means of restructuring power relationships.

Unlike many of the DRM systems currently in place or anticipated, Chaum's technologies respect the *anonymity principle*. This principle is firmly in place in a number of jurisdictions with strong privacy and data protection laws. For example, Australia's national privacy law states that:

> Whenever it is lawful and practicable, individuals must have the option of not identifying themselves when entering transactions with an organization.[70]

Germany has similar provisions in its *Federal Data Protection Act* and its *Teleservices Data Protection Act*:

---

"Tilting at Copyright's Windmill," above note 5 and which is further studied by Jane Bailey in chapter 5.

68 *Ibid*.

69 David Chaum, "Security Without Identification: Transaction Systems to Make Big Brother Obsolete" (1985) 28 Communications of the Association for Computing Machinery 1030 at 1030; David Chaum, "Achieving Electronic Privacy" *Scientific American* (August 1992) at 96, <http://ganges.cs.tcd.ie/mepeirce/Project/Chaum?sciam.html>. Why Chaum's proven techniques (and the many innovations he has subsequently inspired) have experienced failure in the marketplace, despite achieving Weinberg's specification of the original aim of DRM, is an interesting question worthy of pursuit. See <www.anonequity.org>.

70 Australia: *Privacy Act 1988* (Cth), as amended by the *Privacy Amendment (Private Sector) Act 2000* (Cth), Schedule 3, Principle 8 <www.privacy.gov.au/publications/privacy88_030504.pdf>.

> s. 3(a) [*Federal Data Protection Act*] The organisation and choice of data-processing systems shall be guided by the objective of collecting, processing and using as little personal data as possible. In particular, use shall be made of the possibilities of anonymisation and pseudonymisation where possible and where the effort entailed is proportionate to the interests sought to be protected.
>
> s. 4(6) [*Teleservices Data Protection Act*] The provider shall make it possible for the user to utilize and pay for teleservices anonymously or under a pseudonym if this is technically possible and can be accomplished at reasonable effort. The user shall be informed of this possibility.[71]

In addition to explicit provisions such as these, European scholars such as Lee Bygrave have interpreted provisions of the European Community *Data Protection Directive*[72] to include "that persons should be given the opportunity to remain anonymous when entering into transactions with others."[73] According to Bygrave:

---

71 *Federal Data Protection Act of 1990, as amended in 2001* (*Bundesdatenschutzgesetz -)* (Germany), <www.datenschutz-berlin.de/recht/de/bdsg/bdsg01_eng.htm#sec3>; *Information and Communication Services Act of 1997 (Informations- und Kommunikationsdienste-Gesetz – luKDG)* (Germany), Article 2, *Teleservices Data Protection Act (Teledienstedatenschutzgesetz TDDSG)* as amended in 2001, <www.iid.de/iukdg/aktuelles/fassung_tddsg_eng.pdf>.

72 *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] O.J.L 281 at 31 [*DPD*], <http://europa.eu.int/eur-lex/lex/LexUriServ/LexUriServ.do?uri=CELEX:31995L0046:EN:HTML>.

73 Bygrave cites *DPD*, Art. 6(1)(e) and (c), together with Articles 7-8: Bygrave, above note 28 at 429. As well, Bygrave also discussed anonymity as a legal principle in *Data Protection Law: Approaching its Rationale, Logic, and Limits* (The Hague: Kluwer International, 2002) at 346-347 [Bygrave, "Data Protection Law"]. An instantiation of the *DPD* has already found application in Sweden, where DRM-type software was used to record the IP-addresses of file sharers, as well as the alias, the file name, and the server through which the connection was made. Sweden's Data Inspection Board ruled that Antipiratbyrån, Sweden's anti-piracy group, breached *the Personal Data Act* in its hunt for illegal file-sharers (holding that if an IP address can be linked to an individual it is classed as personal information and therefore falls under the *Personal Data Act*). See *The Local* (10 June 2005), <www.thelocal.se/article.php?ID=1581&date=20050610&PHPSESSID=cec0f791dac40515ca2fa14f43d2b762>.

> It is perhaps plausible, though, to argue that Art 6(1)(e) of the EC Directive, in conjunction with the stipulations in Arts 6(1)(c), 7 and 8, already embody a general principle requiring that there be transactional anonymity unless overriding legitimate interests exist to the contrary. More tenuously, such a principle could also be read as implying that active consideration be given to crafting technical solutions for ensuring transactional anonymity.[74]

Applying Bygrave's interpretation to the Canadian context, the anonymity principle is rooted in its broader adjunct, referred to in *PIPEDA* as the "appropriate purposes" principle. According to this principle, "[a]n organization may collect, use or disclose personal information only for purposes that a reasonable person would consider are appropriate in the circumstances."[75] As noted above, since many of the current identification and surveillance features of DRM generally are not necessary, and therefore are generally inappropriate incursions on privacy, there is good reason to think that the "appropriate purposes" principle is applicable to protect the anonymity of those who obtain content through the distribution channels of DRM.

Infusing the anonymity principle into the design of DRM is certainly to be promoted as a matter of public policy. The fact that such techniques are possible and that there is an emerging scholarship on infusing value sensitive design into DRM is encouraging. Given the current state of DRM, these techniques are necessary conditions of placing privacy in the "appropriate balance." Though necessary, it is crucial to recognize that these conditions are by no means sufficient. Given the market failures of privacy-enhancing technologies to date,[76] law must also be used to ensure the appropriate balance. Just as the copyright industries claim that law is needed to protect DRM, law is also needed to protect citizens against

---

74 Bygrave, "Data Protection Law," *ibid.* at 346–47.

75 *PIPEDA*, above note 19, s. 5(3).

76 For example, Digicash – Tim Clark, "Digicash files Chapter 11" *CNET News.com* (4 November 1998) <http://news.com.com/2100-1001-217527.html?legacy=cnet>. For example, Zero-Knowledge Systems – Robert Lemos, "Net users lose a secret-alias tool" *CNET News.com* (4 October 4 2001) <http://news.com.com/2100-1023-273956.html>; Tom Mainelli, "SafeWeb Dumps Free Online Privacy Service" *PC World.com* (21 November 2001), <www.pcworld.com/news/article/0,aid,72466,00.asp>. See generally, Lee A. Bygrave, *Privacy-Enhancing Technologies – Caught between a Rock and a Hard Place,* (2002) 9 Privacy Law & Policy Reporter 135; Ian Goldberg, *Privacy-enhancing technologies for the Internet, II: Five years later*, <www.freehaven.net/anonbib/papers/petfive.pdf>.

DRMs designed to circumvent the anonymity principle where there is no justification for doing so.

The anonymity principle is not new, nor is it unrelated to the domain of intellectual property. The two concepts are not at odds. As Greenleaf pointed out,

> 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 "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.[77]

A government-enabled DRM that does not include counter-measures placing limits on DRM's capacity to collect, meter, monitor, and control information about identifiable individuals threatens the anonymity principle in particular and privacy in general. Silence on these issues in the copyright reform process therefore threatens the concomitant roles that anonymity and privacy play in fostering that which lies at the very heart of copyright: creativity and intellectual achievement.

---

77 Greenleaf, above note 10 at 19. On occasion, copyright law has itself been invoked to protect privacy and secrecy interests. In one well-known case, J.D. Salinger used copyright law to prevent Ian Hamilton from publishing excerpts from his letters in a biography: *J.D. Salinger v. Random House, Inc. and Ian Hamilton*, 818 F.2d 252 (2nd Cir. 1987), <www.bc.edu/bc_org/avp/cas/comm/free_speech/salinger.html>. In another famous decision, the Australian Government used copyright law to prevent the Fairfax newspapers from publishing certain sensitive foreign affairs dossiers: *Commonwealth v. John Fairfax and Sons Ltd.* (1980), 147 C.L.R. 39, <www.austlii.edu.au/au/cases/cth/HCA/1980/44.html>. While these cases reveal that there is no inherent contradiction between copyright and privacy, much depends on whether the person seeking privacy is the owner of the information in question. In any event, it is not copyright but rather one-sided anti-circumvention laws that threaten privacy.

### 2) Individual Access

In addition to the need to place limits on the use of DRM, the concept of an "appropriate balance" is also relevant to the Government's chosen strategy for protecting technical measures — which is to place legal restraints on people's ability to circumvent them. As discussed above , TPMs are a kind of *digital* lock. The proposed restraints on circumvention are a kind of *legal* lock. In the above subsection, my aim was to demonstrate that, since balance is the goal, every lock needs a key. But what happens if there is no digital key? In this brief subsection, I suggest that every digital lock without a key needs a legal locksmith. In other words, laws are necessary to ensure that digital locks can and will be opened when access is justified.

In the copyright context, it is well known that one of the chief concerns about DRM is its ability to lock up a work. The ability to control access has the effect of skewing copyright's delicate balance because the exercise of many of the balancing provisions in the *Copyright Act* are premised on the ability to gain access to the work in the first place.[78] Consequently, the only way to restore balance is to create a positive obligation on the copyright holder to ensure that alternative means of obtaining access to a work remain available.[79] Under this approach, copyright owners would have a positive obligation to provide access-to-a-work when persons or institutions fall within an exception or limitation set out in the *Copyright Act*. Such an obligation might entail the positive obligation to allow access to works in the public domain, or to provide unfettered access-to-works to educational institutions and other organizations that are currently exempted from a number of the provisions in the *Copyright Act*.[80]

Returning to DRM in the privacy context, there are corollary access and control issues stemming from the fair information practices (FIPs) codified in Canadian privacy law. Informational privacy is premised on the idea

---

78 Kerr *et al*., "Tilting at Copyright's Windmill," above note 4 at 77.

79 A "copy-duty," as Lessig has called it: Lessig, "Code and Other Laws," above note 65 at 127. See also Kamiel J. Koelman, "The Protection of Technological Measures vs. the Copyright Limitations" ALAI Congress 2001], <www.ivir.nl/publications/koelman/alaiNY.html>.

80 R.S.C. 1985, c. C-42, ss. 29-30, <http://laws.justice.gc.ca/en/C-42/>. In one variant of this approach, a trusted third party, who holds a copy of the digital work in escrow, could be tasked with resolving access disputes: Dan L. Burk & Julie E. Cohen, "Fair Use Infrastructure for Rights Management Systems" (2001) 15 Harv. J.L. & Tech. 41 at 63 [Burk & Cohen, "Fair Use Infrastructure"], <http://jolt.law.harvard.edu/articles/pdf/15HarvJLTech041.pdf>.

that individuals ought to be able to determine for themselves when, how, and to what extent information about them is communicated.[81] As is the case with access to digital content, an individual's ability to control personal information in some instances depends on that individual's ability to gain access to it in the first place. Canada's privacy legislation contemplates this possibility and posits a general duty upon organizations to ensure that the individual has knowledge of and consents to the collection,[82] and subsequently to provide an individual with access to personal information which has been collected about him or her.[83] Like digital content, personal information that is collected is sometimes locked-up in a technological measure or a DRM database so that an individual has no way of knowing what personal information has been collected, nor any means to access it without hacking past the technology. Obviously, this is problematic from the perspective of informational privacy. An anti-circumvention law that is silent with respect to exceptions permitting circumvention in order to obtain control over or access to one's personal information would therefore enable or facilitate those using DRM to circumvent Canadian privacy law.[84]

Without adequate legal measures re-enabling Canadians' ability to access or control personal information that is under digital lock and key, informational privacy (i.e., the ability for Canadians to determine when, how, and to what extent information about them is communicated), will be seriously undermined.[85]

---

81 See for example, Alan F. Westin, *Privacy and Freedom*, (New York: Atheneum, 1970) at 322.

82 More specifically, Principle 3 in Schedule 1 of *PIPEDA*, above note 19, states that: "The knowledge and consent of the individual are required for the collection, use, or disclosure of personal information, except where inappropriate."

83 More specifically, Principle 9 in Schedule 1 of *PIPEDA*, above note 19, states that: "Upon request, an individual shall be informed of the existence, use, and disclosure of his or her personal information and shall be given access to that information. An individual shall be able to challenge the accuracy and completeness of the information and have it amended as appropriate."

84 *PIPEDA*, above note 19, s. 6 & s. 10; OECD, above note 19, ss. 2 & 7.

85 One might argue that Canadian privacy law would *not* be undermined because *PIPEDA* and substantially similar legislation already allow organizations to engage in the collection of personal information and monitoring so long as they define the purposes for doing so and obtain consent for such purposes. As I argue below in Part E, the digital lock-up of personal information could undermine Canadian privacy law given the requirement in section 5(3) [restricting the collection, use, or disclosure to appropriate purposes determined on a "reasonable person" standard] in conjunction with the higher statutory threshold for consent.

### 3) DRM Licences

Having canvassed two of the key public policy issues arising from DRM's surveillance capabilities and its ability put a digital lock (and a digital veil) around the personal information it collects, it is also crucial to address issues arising from its legal component, the contractual licence.

Like other contractual devices, an Intellectual Property (IP) licence allows copyright holders to set the terms of use for their products. However, in the DRM context,[86] intelligent agent technologies[87] facilitate the automatic "negotiation" [88] of contractual licences between content providers and users, as well the plethora of informational transactions that are generated as a result of them.

In an automated environment, most informational transactions take place invisibly through software exchanges between machines, about which few humans are aware and fewer still have the technical expertise to alter. Bits and bytes of data, not to mention various forms of personal information, are collected and inconspicuously interchanged without human intervention and often without knowledge or consent. Automation[89] therefore exacerbates an already problematic inequality in the bargaining power between the licencors and licencees resulting from standard form agreements[90] and mass market licences.[91] The combination of TPMs and contracts in this manner could

---

86 Bechtold, above note 27 at 614.

87 For a general discussion of the legal issues surrounding intelligent agents, see Ian R. Kerr, "Spirits in the Material World" (1999) 22 Dalhousie Law Journal 189.

88 The "scare quotes" used here are intentional and meant to indicate what I think is a misleading if not false use of the term "negotiation." The entire point of this sub-section is to indicate that there is no negotiation taking place, and that DRM and the terms of its use are being unilaterally imposed on people through the device of DRM.

89 Automation is a key aspect of the DRM strategy. The automation of transactions — removing human beings from decision-making processes — enables and facilitates the use of one-sided terms in a *contrat d'adhesion*. The success of "Rights Management" depends on it.

90 See W. David Slawson, "Standard Form Contracts and Democratic Control of Lawmaking Power" (1971) 84 Harv. L. Rev. 529 at 556; Friedrich Kessler, "Contracts of Adhesion: Some Thoughts About Freedom of Contract" (1943) 43 Columbia L.R. 629 [Kessler, "Contracts of Adhesion"]; George Gluck, "Standard Form Contracts: The Contract Theory Reconsidered" (1979) 28 Int'l & Comp. L.Q. 72.

91 Garry L. Founds, "Shrinkwrap and Clickwrap Agreements: 2B or Not 2B?" (1999) 52 Fed. Comm. L.J. 99; Daniel B. Ravicher, "Facilitating Collaborative Software Development: The Enforceability of Mass-Market Public Software Licenses" (2000) 5 Va. J.L. & Tech. 11.

therefore lead to unfair transactions. As three of the world's leading scholars in the field have expressed:

> Are we heading for a world in which each and every use of information is dictated by *fully automated systems*? A world in which every information product carries with itself its own unerasable, non-overridable licensing conditions? A world in which what is allowed and what is not, is no longer decided by the law but by computer code?[92]
>
> ...
>
> Where technological constraints substitute for legal constraints, control over the design of information rights is shifted into the hands of private parties, who may or may not honor the public policies that animate public access doctrines such as fair use. Rights holders can effectively write their own intellectual property statute in computer code.[93]

End user licences are becoming the rule and content providers the rulers. With increasing frequency, the terms of these licences are used to override existing copyright limitations.[94] As Guibault aptly articulates:

> Concerns arise from the possibility that an unbridled use of technological measures coupled with anti-circumvention legislation and contractual practices would permit rights owners to extend their rights far beyond the bounds of the copyright regime, to the detriment of users and the free flow of information. The copyright bargain reached between granting authors protection for their works and encouraging the free flow of information would be put in serious jeopardy if, irrespective of the copyright rules, rights owners were able to impose their terms and conditions of use through standard form contracts with complete impunity. If this were the case, the copyright regime would succumb to mass-market licenses and technological measures. Unless the legislator clarifies the issue, these concerns may become all too real with the gradual implementation of electronic copyright management systems, whose works are based on technology and con-

92 See Hugenholtz, "Copyright, Contract and Code" above note 30 at 86–87.

93 Burk & Cohen, "Fair Use Infrastructure" above note 80 at 51.

94 See Hugenholtz, "Copyright, Contract and Code" above note 30 at 80. See also, Lucie Guibault, "Contracts and Copyright Exemptions" in Bernt Hugenholtz (ed), *Copyright and Electronic Commerce: Legal Aspects of Electronic Copyright Management* (The Hague: Kluwer Law International, 2000) at 125; Jerome H. Reichman & Jonathan A. Franklin, "Privately Legislated Intellectual Property Rights: Reconciling Freedom of Contract with Public Good Uses of Information" 14 U. Pa. L. Rev. 875.

> tractual relations, with the generalization of mass-market licenses as the main vehicle for transactions in information ..."[95]

The above analysis applies *mutatis mutandis* in the privacy context. An unbridled use of TPM with anti-circumvention legislation and contractual practices would permit content owners to extend their surveillance and personal information collection practices far beyond the bounds of what might otherwise be permitted by Canadian privacy law, to the detriment of everyone who uses DRM.[96] Like copyright, privacy law's compromise between the needs of organizations[97] 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.

Allowing TPMs and DRM licences to circumvent the privacy rights of individuals without appropriate counter-measures will undermine the "appropriate balance" that the Government has undertaken to achieve in its copyright reform initiative.[98] Consequently, there is value in contem-

---

95 Guibault, *ibid.* at 160.

96 Given that the proposed copyright reforms are part of a global initiative that would enable and facilitate the development of DRM as *the* secure global distribution channel for all digital content, it is arguable that this will affect everyone.

97 To collect, use, or disclose personal information for purposes that a reasonable person would consider appropriate in the circumstances: *PIPEDA* above note 19, s. 3.

98 See *Statement*, above note 12: "One of the public policy principles underlying the *Act* is the need to maintain an appropriate balance between the *rights* of copyright owners and the *needs* of [...] users." As Jane Bailey has indicated, it is interesting to note the Government's decision to frame the balance in terms of "owners rights vs. the needs of users." Framing the policy approach in this manner is unjustifiable given that the *Copyright Act* clearly grants "rights" to users (rather than mere needs) and rights of access to and use of information form part of the constitutionally enshrined right to freedom of expression: see chapter 5. *A fortiori*, Bailey's critique is bolstered in the privacy context where the legislation itself clearly stipulates in the "Purpose" section the very opposite way of framing the issue:

> The purpose of this Part is to establish, in an era in which technology increasingly facilitates the circulation and exchange of information, rules to govern the collection, use and disclosure of personal information in a manner that recognizes *the right of privacy of individuals* with respect to their personal information and *the need of organizations* to collect, use or disclose personal information for purposes that a reasonable person would consider appropriate in the circumstances.

[*PIPEDA*, above note 19, s. 3 (emphasis added)].

plating basic common law principles and their potential applicability for setting appropriate limits on DRM's ability to exploit the law of contract. Though a detailed account of contract law theory is certainly out of place, a succinct discussion regarding some limits on "freedom to contract" merits some attention.

As any first year student will attest, the law of contract commences with the idea of "freedom to contract" — that "the Chancery mends no man's bargain"[99] — and then systematically proceeds to undermine the idea through various doctrines.[100] Waddams states that, "[p]erhaps the most open opposition to the principle of the free enforceability of contractual agreements has been the striking down of agreements on the ground that they are contrary to public policy."[101] While the courts generally tend to avoid interfering with individual bargains, they will in some instances render void a contract that is illegal, whether because it: (i) contravenes a statute, or (ii) is inconsistent with public policy.

Does DRM surveillance contravene *PIPEDA* or its provincial equivalents?[102] To date, the Commissioner has issued no findings directly on this issue. And given that there is no single technological standard for DRM and that different providers offer different terms of use, the more appropriate question is whether DRM surveillance *could* contravene the legislation. Although the answer to this question involves some speculation, there are good grounds for answering in the affirmative. At least, that is what the Privacy Commissioner of Canada thinks. Interested in the privacy implications of DRM for some time, she has expressed her concerns as follows:

> We would, naturally, have serious concerns about the design and deployment of any technology that facilitated the fine-grained surveillance of individuals without their informed consent. We would certainly have concerns about any commercial enterprise in Canada that deployed privacy-invasive DRM technologies in contravention of the

---

99 Lord Nottingham in *Maynard v. Moseley* (1676) 3 Swans. 651 at para. 655.

100 Including, "capacity," "*consensus ad idem*," "consideration," "privity," "duress," "undue influence," "unconscionability," "illegality," and "public policy."

101 Stephen Waddams, *The Law of Contracts,* 4th ed. (Toronto: Emond Montgomery Publications, 1999) at 399 [Waddams, *The Law of Contracts*].

102 Quebec: *Act respecting the protection of personal information in the private sector,* R.S.Q., c. P-39-1, <www.canlii.org/qc/laws/sta/p-39.1/20040323/whole.html>; British Columbia: *Personal Information Protection Act,* S.B.C. 2003, c. 63, <www.qp.gov.bc.ca/statreg/stat/P/03063_01.htm>; Alberta: *Personal Information Protection Act*, S.A. 2003, c. P-6.5, <www.canlii.org/ab/laws/sta/p-6.5/20050318/whole.html>.

> provisions of the *Personal Information Protection and Electronic Documents Act* (*PIPEDA*) and the fair information practices underlying it.[103]

The above passage, though not intended as dispositive, certainly lends credence to the possibility that a DRM surveillance device engaging in excessive monitoring or collection would contravene *PIPEDA*.[104] The Commissioner went on in that same correspondence to suggest that DRM fits within a class of "similar surveillance issues, including RFID tags, computer spyware, and 'lawful access' proposals."[105]

If this is so, then there is good reason to believe that courts might set aside a DRM licence aiming to circumvent *PIPEDA* on the grounds of statutory illegality. After all, as the Supreme Court of Canada ruled long ago, "[i]t would be a curious state of the law if, after the Legislature had prohibited a transaction, parties could enter into it, and, in defiance of the law, compel the courts to enforce and give effect to their illegal transaction."[106]

Even if a particular instance of DRM surveillance would not be found to contravene *PIPEDA* — say, for example, the information collected, used,

---

103 Letter to Phillipa Lawson and Alex Cameron from Privacy Commissioner of Canada, (24 November 2004), <www.cippic.ca/en/projects-cases/copyright-law-reform/LF%20Privacy%20Commissioner%20re%20copyright%20and%20DRM%20&%20TPM%20-%20Nove%2024%2004.pdf> [Letter]. I am indebted to Alex Cameron for alerting me to the existence of this letter.

104 However, everything would very much depend on how the DRM's collection process was set-up. Consider, for example, the video camera surveillance system used in *Eastmond v. CPR*, [2004] F.C.J. No. 1043. CPR used video cameras to record activities in its Toronto yard, keeping the recordings in a locked area in order to ensure that they were never viewed by anyone unless an incident took place in the yard. If no incidents were reported, the recordings were automatically destroyed within 96 hours. According to the court, no "collection" of personal information occurred until such time as an incident was reported and the videotape viewed. In other words, automated systems that do not involve human observers are not collecting information and therefore not in violation of *PIPEDA*. This decision, if upheld, could have significant ramifications for DRM, since its automation usually does not require human intervention. For a further discussion of this decision and its potential impact on the regulation of DRM monitoring, see Cameron, "Digital Rights Management," above note 38.

105 Jennifer Stoddart, Letter, above note 103. It should be noted that Commissioner Stoddart was careful to disclose her intention to "maintain the neutrality and impartiality expected of a national ombudsman, in order to be able to address complaints fairly and with credibility. This can sometimes mean neither endorsing nor condemning specific technologies and standards — particularly when not all the facts are known."

106 *Bank of Toronto v. Perkins* (1893), 8 S.C.R. 603, Ritchie C.J.

or disclosed did not require consent under the *Act*[107] — a court might still find the terms of use in an end user licence seeking to permit DRM surveillance to be void for public policy.[108] Though notoriously vague, and although the inclination of courts is to defer to the Legislature on such matters, the test for illegality (whether by statute or at common law) seeks to determine whether the contract in question would offend the basis of legal order, as founded upon justice, legality, and morality.[109] As such, even if an argument against DRM surveillance cannot be made under the rubric of statutory illegality, a DRM licence premised on excessive collection of monitoring could still be void on public policy grounds, pursuant to the test for common law illegality.[110]

Admittedly, it is more difficult to imagine such a finding. After all, courts have been willing to enforce other contracts involving privacy-invasive surveillance. For example, contracts have been enforced involving private investigators,[111] strippers,[112] talk show guests,[113] and even reality television show contestants.[114] There are however, important differences between each of these and DRM surveillance.

Private investigators, while their role is to engage in surreptitious surveillance, are not usually able to penetrate a person's home, hard drive, or other intellectual assets such as PDAs, iPods, or online journals. Their surveillance is usually limited to that which is publicly observable. While some people believe that strip clubs are immoral[115] or that the sex-industry

---

107 For example, Principle 4.3 stipulates that "... security reasons may make it impossible or impractical to seek consent." *PIPEDA* above note 19, Sch. 1, cl. 4.3.

108 This doctrine is sometimes referred to as "common law illegality." Gerald H. L. Fridman, *The Law of Contract in Canada,* 4th ed. (Scarborough, ON: Carswell, 1999) at 390–436 [Fridman, *The Law of Contract*].

109 Fridman, *ibid*. at 391.

110 *Egerton v. Brownlow* (1853), 4 H.L. Cas. 1, 10 E.R. 359 at 437 (H.L.), stating that, "no subject can lawfully do that which has a tendency to be injurious to the public or against the public good which may be termed, as it sometimes has been, the policy of the law or public policy in relation to the administration of law."

111 *Shawn Ripplinger v. Sue Edwards* (1996), 140 Sask. R. 230 (QB); *Great Atlantic & Pacific Co. of Canada v. U.F.C.W., Locals 175 & 633 — In the Matter of the Grievance of G. Konefal* (2004), L.V.I. 3446-2 (OAB).

112 *Suave v. Minister of National Revenue* (1995), 132 D.L.R. (4th) 114 (F.C.A.); *Menard v. Tasnadi*, [1987] B.C.J. No. 66 (S.C.).

113 *Sheila C. v. Povich* (2004), 781 N.Y.S. 2d 342.

114 *SEG, Inc. v. Stillman* (2003), Cal. App. Unpub. Lexis 5067. I owe these excellent examples to Daniel Solove.

115 Chris Bruckert & Martin Dufresne, "Re-Configuring the Margins: Taking the Regulatory Context of Ottawa Strip Clubs, 1974–2000" (2002) 17:1 Canadian

engages in practices resulting in the systemic oppression of women,[116] the nature of the surveillance is different, from a privacy perspective, since the individuals in question are fully aware of the privacy invasion.[117] The same is generally true for talk show guests and reality TV contestants. In the latter instances, the whole point of the contract is remuneration in exchange for some kind of exposure that would otherwise be private. While there may be issues about whether consent is genuine,[118] the nature of these privacy invasions are known to the parties and, eventually, felt or understood. Intellectual privacy, as described above, is not really at stake here. The same is not true of DRM surveillance. The subject matter of these contracts is the purchase of intellectual content such as books, CDs, movies, and magazines. These materials are usually consumed in private. Any privacy invasive modalities that occur in the distribution of these products are clearly incidental to the root of the bargain. This creates an additional set of public policy concerns when it comes to the enforceability of DRM licences, the fine print of which seeks to justify the invasive interaction.

Would a DRM licence that permitted excessive monitoring or collection be contrary to public policy? Interestingly, in response to an informal letter posing a public policy question about the potential impact on privacy of DRM technologies, the Privacy Commissioner of Canada recently indicated that:

---

Journal of Law & Society 69; Nova Sweet & Richard Tewksbury, "What's a Nice Girl Like You Doing in a Place Like This? Pathways to a Career in Stripping" (2000) 20:3 Sociological Spectrum 325.

116 Susan Cole, *Pornography and the Sex Crisis* (Toronto: Second Story Press, 1992); Catherine MacKinnon, *Only Words* (Cambridge, Mass.: Harvard University Press, 1993); Andrea Dworkin, *Pornography: Men Possessing Women*, (London: The Women's Press, 1981).

117 In fact, it is for this reason that the humiliation and degradation that goes along with being required to undress or perform sexual acts in front of people or cameras usually requires some sort of psychological detachment or desensitization akin to that experienced by those subject to Big Brother's telescreen in Orwell's *1984* (George Orwell, *1984*, (London: Secker & Warburg, 1949)). DRM surveillance and the dossiers of information collected thereby are of a very different nature, more similar to the surveillance experienced by Joseph K. in Kafka's *The Trial* (Franz Kafka, *The Trial* (New York: Knopf, 1957)). For further reflections on these differences, see Daniel J. Solove, "Privacy and Power: Computer Databases and Metaphors for Information Privacy" (2001) 53 Stan. L. Rev. 1393.

118 The feminist literature cited above note 116 demonstrates well that the law of contract, and its doctrine of "consent," both of which are premised on liberal individualism, are not the appropriate constructs for solving some of these social issues.

> We would oppose legislation or legislative amendments that conferred unjustified privacy-invasive surveillance powers upon digital copyright holders. However, we have not as yet been consulted by either Heritage Canada or Industry Canada officials regarding the proposed legislation ....[119]

Although some consultation has occurred since the Privacy Commissioner wrote these words, the failure of Canadian Heritage and Industry Canada to engage in earlier dialogue, let alone a collaborative effort with the Privacy Commissioner, is especially interesting in light of the fact that *PIPEDA,* the legislation for which she has oversight, appears to be *lex specialis* to the *Copyright Act*. Pursuant to section 4(3), the privacy requirements of *PIPEDA* apply despite any provision in any other *Act,* unless the other *Act* expressly declares that its provision operates notwithstanding.[120] When one considers that Bill C-60 is silent on this issue, it would seem that the requirements of *PIPEDA* would prevail, further buttressing the claim that excessive DRM monitoring or collection would be contrary to public policy.

## E. FREEDOM FROM CONTRACT

My thesis should by now be clear. If anti-circumvention laws are to "ensure that Canadians' privacy rights are not reduced or undermined,"[121] then the amendments to the *Copyright Act* must include a different kind of anti-circumvention provision. In addition to prohibiting the circumvention of TPMs for infringing purposes, there must be a balancing counter-measure that expressly prohibits the use of DRM to circumvent the protection of Canadian privacy law. "Appropriate balance," in this sense, requires a legal lock aimed against organizations that would use TPMs, the proposed anti-circumvention law, and the law of contract as a means of hacking past *PIPEDA* or its provincial equivalents. In order to understand why this is so, it is necessary describe the chief tool in the DRM hack-back-pack: contractual consent.

---

119 See Letter, above note 103.

120 *PIPEDA,* above note 19, s. 4(3).

121 *This is an explicit promise made by the Government of Canada*: Copyright Reform Process — Frequently Asked Questions, <http://strategis.ic.gc.ca/epic/internet/incrp-prda.nsf/en/rp01143e.html>.

When it comes to DRM and privacy, there are two kinds of consent.[122] The first refers to the consent required to give rise to the DRM contractual licence. DRM consent is *merely* contractual consent. The second refers to the threshold of consent that may be required to satisfy FIPs. FIPs consent is, in most circumstances,[123] a much more robust form of statutory consent. It is crucial to note the distinction. They are not the same.[124] The reason for the need to draw a laser-bright line between them was articulated in the preceding section on DRM licenses. Not to put too fine a point on it, here is how three of the leading U.S. privacy scholars have put it:

Daniel Solove:

> The law currently does not provide meaningful ability to refuse to consent to relinquish information.
>
> ...
>
> 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 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.[125]

Paul Schwartz:

> To give an example of an autonomy trap in cyberspace, the act of clicking through a "consent" screen on a Web site may be considered by some observers to be an exercise of self-reliant choice. Yet, this screen can contain boilerplate language that permits all further processing and transmission of one's personal data. Even without a consent screen, some Web sites place consent boilerplate within a "privacy statement"

---

122 I am not referring to true consent, implied consent, or informed consent, though all of those concepts are applicable.

123 As discussed below, FIPs require knowledge and consent in many collections, uses, and disclosures of personal information and, in the case of sensitive information, a standard closer to informed consent. Often there are exceptions for situations where it is not possible of appropriate to obtain consent.

124 Though in certain circumstances one might satisfy the other.

125 Daniel J. Solove, *The Digital Person: Technology and Privacy in the Information Age* (New York: NYU Press, 2004) at 82–85.

> on their home page or elsewhere on their site. ... This language presents the conditions for data processing on a take-it-or-leave-it basis. It seeks to create the legal fiction that all who visit this Web site have expressed informed consent to its data processing practices.[126]

Julie Cohen:

> The single greatest obstacle to effective legal protection of privacy of intellectual consumption is not imperfect fit with the available legal theories, but the fact that the available theory gives way to contract in many, if not all circumstances.[127]

As each of these three outstanding scholars states in his or her own way, 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."[128] 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."[129] In some instances, and privacy is certainly one of them, what people need is freedom *from* contract.[130]

The idea that there is sometimes a need to protect people *from* the private device of contract and its low threshold for consent is not completely new. Consumer protection legislation provides an excellent example.[131] Although the stated purpose of Canada's federal privacy legislation[132] involves balancing the needs of organizations to collect personal information against the privacy rights of individuals, many believe that the failure of the market to protect privacy through "self-regulation" is the entire basis for enacting *PIPEDA* and substantially similar provincial leg-

126 Paul M. Schwartz, "Privacy and Democracy in Cyberspace" (1999) 52 Vand. L. Rev. 1609, <http://papers.ssrn.com/sol3/Delivery.cfm/000120306.pdf?abstractid=205449&mirid=1> at 1661.

127 Cohen, "DRM and Privacy," above note 17 at 605.

128 Kessler, "Contracts of Adhesion," above note 90 at 632.

129 I borrow this way of characterizing things from Ann Bartow.

130 This is in fact one of the reasons for consumer protection legislation and privacy legislation such as *PIPEDA*.

131 See for example, *Consumer Protection Act*, R.S.O. 2002, c. C. 30, Sch. A. <www.canlii.org/on/laws/sta/c-31/20050511/whole.html>; *Consumer Protection Act*, R.S.B.C. 1996, c. 69, <www.qp.gov.bc.ca/statreg/stat/C/96069_01.htm>; Andrew Morrison, "When Voluntary is not really Voluntary: Contractual Aspects of Voluntary Codes" (1997) 3 Appeal 34.

132 *PIPEDA*, above note 19, s. 3.

islation.[133] Using *PIPEDA* as the model, there are at least three elements built into the legislation as counter-measures to the low threshold of contractual consent and the one-sided nature of standard form agreements: (i) a appropriate purpose requirement; (ii) a higher statutory threshold for consent; (iii) a "refusal to deal" clause.

### 1) Appropriate Purpose

Section 5(3) of *PIPEDA* uses the common law construct of the "reasonable person" as an essential limiting factor against what the private law might otherwise deem to be a consensual collection of personal information:

> An organization may collect, use or disclose personal information only for purposes that a reasonable person would consider are appropriate in the circumstances. [134]

According to this section, even if a person carefully considers and then expressly consents to the collection of personal information, her consent will not justify collection if its purpose for the collection is said to be unreasonable. This section places constraints on the law of contract and the role of consent. If the purposes for collection, use, or disclosure are deemed unreasonable, the fact that the information subject consented will not justify its collection, use, or disclosure.[135] This provision therefore offers protections not provided by the common law. When parties enter into a contract, so long as there is fairness during the bargaining process, the courts are loath to determine whether the bargain between the parties is reasonable.[136] Not so with the application of this section of the legisla-

---

133 That is, in the age of technology, self-regulation will not suffice. See Stephanie Perrin *et al.*, *The Personal Information Protection and Electronic Documents Act: An Annotated Guide* (Toronto: Irwin Law, 2001) at 5 [Perrin, *Personal Information Protection]*: "But by 1994, Bruce Phillips had reached the conclusion that self-regulation was not enough, and he started calling on the government to legislate broadly at the national level in his 1993-1994 report ...."

134 *PIPEDA,* above note 19, s. 5(3).

135 See, for example *Company asks for customer's SIN as a matter of policy*, (5 November 2001), *PIPED Act* Case Summary #22, <www.privcom.gc.ca/cf-dc/2001/cf-dc_011105_02_e.asp> [*PIPED Act* Case Summary #22, "*Company asks for customer's SIN*"]. See also *Reasonable and the Reasonable Person within the Scope of PIPEDA*, Nymity Inc., <www.nymity.com/faq/reasonable_and_the_reasonable_person.asp>.

136 *Miller v. Lavoie* (1966), 63 W.W.R. 359 at 365 (B.C.S.C.).

tion. Here the reasonableness of the purposes for collection, use, or disclosure is determinative.

### 2) Higher Statutory Threshold for Consent

In addition to the constraints placed on contractual consent set out in section 5(3), Principle 4.3 of Schedule 1 in *PIPEDA* generally provides for a higher threshold of consent than that usually required by the law of contract. Unlike the weaker party to a contract, who clicks through a standard commercial agreement, the data subject will not simply be deemed to consent. She or he must usually be said to consent *knowingly*:

> The knowledge and consent of the individual are required for the collection, use, or disclosure of personal information, except where inappropriate.[137]

A further provision has been put in place to ensure that the consent has been obtained in a meaningful way, generally requiring that organizations communicate the purposes for collection, so that the person will reasonably know and understand how the information will be collected, used, or disclosed.[138]

Yet another means of ensuring a high threshold for consent is achieved by virtue of the fact that *PIPEDA* contemplates different forms of consent, depending on the nature of the information and its sensitivity.[139] Information said to be "sensitive" will generally require more detailed and in some instances express consent.[140] The rationale for this is that "in obtaining consent, the reasonable expectations of the individual are also rel-

---

137 *PIPEDA,* above note 19, Sch. 1, cl. 4.3.

138 *Ibid*. Sch. 1, cl. 4.3.2. See, for example *Bank adopts sweeping changes to its information collection practices,* (30 September 2002) *PIPED Act* Case Summary #97, <www.privcom.gc.ca/cf-dc/2002/cf-dc_020930_e.asp>. It is crucial to note that a substantial number of limits on the high threshold of consent have been placed in s. 7 of the Act. For example, s. 7(1)(b) states an organization may collect personal information without the knowledge or consent of the individual 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." This provision was cited in the *Eastmond v. Canadian Pacific Railway*, [2004] F.C.J. No. 1043, regarding Principle 4.3, where video surveillance was said to be appropriate by J. Lemieux. A factor in the decision was that the camera was minimally invasive, and was only looked at if there was a triggering incident. After 96 hours the video was deleted (para. 188).

139 *PIPEDA,* above note 19, Sch. 1, cl. 4.3.4.

140 *Ibid*.

evant."[141] Note that this is a different "reasonableness" requirement than the one discussed in the preceding section. There, the reasonableness had to do with an organization's purposes for collection, use, or disclosure. Here, reasonableness has to do with the information subject's actions and whether consent can truly be inferred from them.[142]

One further difference between contractual consent and the consent requirement in *PIPEDA* is that only in the latter can consent be withdrawn with impunity.[143] This signals that, in the privacy context, consent is an ongoing obligation. To some extent, it empowers the weaker party in the transaction to change her or his mind. It is not all-or-nothing. It is not take-it-or-leave it. The law of contracts, on the other hand, is promissory in nature[144] and is premised on the notion of detrimental reliance.[145] Withdrawing consent once a contract has been formed usually amounts to a breach of contract or an anticipatory repudiation.

Even this brief snapshot should illustrate that the concept and application of consent in Canadian privacy law is nuanced and difficult.[146] Among other things, the consent requirement will vary based on the purpose of the collection, use, or disclosure of the information, its sensitivity, the reasonable expectation of the parties, and the reasonableness of the information subject's actions in and around the collection process. Generally, the threshold is significantly higher in the privacy context than in contract law.

The lower threshold of contractual consent is too blunt a tool for privacy law. It therefore ought not to be used to undermine FIPs, nor to data-mine or conduct surveillance against those who use DRM-delivered intellectual content. As the following subsection indicates, this point was not overlooked by those who enacted Canada's privacy legislation.

---

141 *Ibid.,* Sch. 1, cl. 4.3.5.

142 According to the Privacy Commissioner, "[i]mplied consent arises where consent may reasonably be inferred from the actions or inactions of the individual." *Telecommunications company does not improperly collect or use employee statistics* (14 April 2003) *PIPED Act* Case Summary #153, <www.privcom.gc.ca/cf-dc/2003/cf-dc_030414_3_e.asp>.

143 *PIPEDA,* above note 19, Sch. 1, cl. 4.3.8. Note that the ability to withdraw consent is, however, subject to legal or contractual restrictions and reasonable notice.

144 Fridman, *The Law of Contract,* above note 108 at 1 & 3.

145 Waddams, *The Law of Contracts*, above note 101 at 193.

146 See for example, *Air Canada allows 1% of Aeroplan membership to "opt out" of information sharing practices,* (11 March 2002), *PIPED Act* Case Summary #42, <www.privcom.gc.ca/cf-dc/cf-dc_020320_e.asp>.

### 3) "Refusal to Deal" Clause[147]

A third *PIPEDA* provision that highlights the need to distinguish between DRM's contractual consent and the higher threshold in FIPs consent is Principle 4.3.3, which states that:

> An 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 fulfill the explicitly specified, and legitimate purposes.[148]

This provision is a clear and obvious limitation on the take-it-or-leave-it approach of DRM's contractual consent, and has been affirmed in several decisions. In one instance,[149] a telecommunications company tried to force a customer to provide her social insurance number (SIN) as a prerequisite to Internet access. Though willing to allow organizations to request SIN for identification purposes if they clearly indicate that doing so is optional, the Privacy Commissioner ruled against the company's "No SIN, no connection" policy.[150] As some experts have described, "The message is clear: if you are planning to deny a service to someone for failure to provide information, the information must be necessary to fulfill a legitimate and specific purpose, not an overly broad or inflated one."[151]

Taken together, the reasonable purpose requirement, *PIPEDA*'s higher consent threshold, and the "refusal to deal" clause are all meant to provide protections to individuals which "self-regulation" through the device of contract would not achieve. Should DRM licences be permitted to circumvent these protections? Should consumers, who often have no idea what is at stake, be allowed to "contract-away" these protections unknowingly? And should anti-circumvention laws be drafted — as is currently contemplated in Canada — in a manner that permits and protects privacy-invasive TPMs and DRMs, which could operate in breach of *PIPEDA* or other operative statutes? Perhaps the dictum of the Supreme Court of Canada bears repeating: "[i]t would be a curious state of the law if, after the Legislature had prohibited a transaction, parties could enter into it, and, in defiance of the law,

---

147 This clause was dubbed the "refusal to deal clause" by the CSA Committee and was the subject of much debate: Perrin *et al*., above note 133 at 25.

148 *PIPEDA,* above note 19, Sch. 1, cl. 4.3.3.

149 *PIPED Act Case Summary #22*, "*Company asks for customer's SIN,*" above note 135.

150 See Barbara McIsaac, Rick Shields, & Kris Klein, *The Law of Privacy in Canada*, (Toronto: Carswell, 2004) at 4–40.

151 Perrin *et al*, above note 133 at 27.

compel the courts to enforce and give effect to their illegal transaction."[152] Privacy law is meant, in some instances, to provide *freedom from contract*.

## F. THE SOUNDS OF SILENCE

Having examined in some detail the prospect of DRM and its potential impact on privacy, it is alarming to see that Canada's proposals for copyright reform are completely silent on the issue. According to Bill C-60, the proposed anti-circumvention law will protect technological measures and enable DRMs in the following manner:

> 34.01(1) The owner of copyright in a work … is … entitled to all remedies by way of injunction, damages … for the infringement of a right against a person who, without the consent of the copyright owner, knowingly removes or alters any rights management information in electronic form that is attached to or embodied in any material form of the work … and knows, or ought to know, that the removal or alteration will facilitate or conceal any infringement of the owner's copyright.[153]

> 34.02(1) An owner of copyright in a work … and a holder of moral rights in respect of a work … are … entitled to all remedies by way of injunction … for the infringement of a right against a person who, without the consent of the copyright owner or moral rights holder, circumvents, removes or in any way renders ineffective a technological measure protecting any material form of the work … for the purpose of an act that is an infringement of the copyright in it or the moral rights in respect of it or for the purpose of making a copy referred to in subsection 80(1).[154]

Not a single word, let alone appropriate counter-measures, has been contemplated in connection with the implications of DRM for privacy. *Not one word*.

All that is proposed is a set of one-sided deeming provisions that expand the ambit of copyrights by treating acts of circumvention as though they are acts of infringement. The effect of these paracopyright provisions will be to further expand the law of copyright so that it includes certain

---

152 Ritchie C.J, above note 106.
153 *Copyright Amendment*, above note 5, s. 34.01.
154 *Ibid*., s. 34.02.

*acts* that have nothing to do with copying.[155] The activities that might soon be said to constitute an infringement include "circumvent[ing], remov[ing] or in any way render[ing] ineffective a technological measure protecting any material form of the work"[156] and "knowingly remov[ing] or alter[ing] any rights management information in electronic form that is attached to or embodied in any material form of the work."[157]

By treating the circumvention of a TPM or the alteration of RMI (under certain circumstances) *as though* they are copyright infringements, these provisions place new restrictions on people's ability to examine, investigate, or interact with the technologies destined to become a global distribution channel for delivering digital content. Some academics are concerned that such restrictions could interfere with the security community's "freedom-to-tinker," which will have a chilling effect on important research in cryptography and other areas.[158]

Of course, there are other legitimate reasons to tinker. Unless these are articulated and distinguished from illegitimate circumventions in the proposed anti-circumvention provisions, it may be practically impossible to distinguish "legitimate" from "infringing purposes." A relevant example for present purposes is circumvention or alteration for personal information protection purposes. Data protection legislation is premised on the idea that individuals should be able to gain access to personal information collected about them,[159] as well as the need for "openness" in organizations about the policies and practices relating to their management of others' personal information.[160] In the case of DRM, often that information is not generated or stored at some organization's facilities but by software that is in fact housed on the data subject's own computer.

So, I might want to tinker with a DRM — to decrypt or otherwise unlock its hidden code; to hack it — not because I wish to interfere with its

---

155 When those acts can be tied to an "infringing purpose." Tying circumvention to infringing purposes is certainly an improvement over *DMCA*-style legislation, which captures circumventions that have nothing to do with infringement whatsoever: *DMCA*, above note 2. For a further analysis of this approach, see chapter 4.

156 *Copyright Amendment*, above note 5, s. 34.02.

157 *Ibid*., s. 34.01.

158 See for example, Edward W. Felten, "Freedom to Tinker," <www.freedom-to-tinker.com>; Scott A. Craver et al., "Reading Between the Lines: Lessons from the SDMI Challenge" (2001) Proc. Of 10th USENIX Security Symposium, <www.usenix.org/events/sec01/craver.pdf>.

159 See *PIPEDA,* above note 19, Sch. 1, cl. 4.9.

160 *Ibid*.

copyright enforcement function but because I am interested in knowing whether excessive collection or monitoring is taking place. Perhaps I even suspect it, in which case my purpose in circumventing is to achieve transparency. I am trying to see what kind of personal information a particular technology is scraping away from me or my computer every time I interact with it.[161] Just as organizations might not, in some circumstances, be in a position to obtain consent in advance when collecting personal information (say, for security purposes), so too might it be necessary for individuals to circumvent or remove personal information without permission in order to secure their personal information against illegitimate collection, use, and disclosure.

Are people permitted to unlock the devices wrapped around the products that they have legally purchased in order to investigate what is happening with their personal information? Under what circumstances? With what limitations? What if doing so undermines or defeats an access control mechanism? What remedies are available if the DRM *is* being used in a manner contrary to privacy law? This list of questions goes on and on. And, yet, none of them is addressed in the current proposals for copyright reform. If balanced legislation is the goal, then silence simply will not do. The proposed anti-circumvention provision must specifically stipulate the elements of an illegal circumvention in a manner that expressly distinguishes "infringing activities" from other activities such as security research or activities undertaken simply to obtain access to personal information that is being collected by a DRM, or to otherwise exercise control over personal information consistent with the rights guaranteed by FIPs and by privacy law.[162]

Ironically, in spite of its renown as the world's most unbalanced, one-sided, DRM-maximalist legislation in force, even the *DMCA* purports to address some of the above concerns. The *DMCA* expressly permits the disablement of monitoring mechanisms tied to access controls so long as the following cumulative conditions are met:

1) the access controls, in the normal course of operation, collect or disseminate "personally identifiable information" about the online activities of a person who seeks access to the protected work;
2) conspicuous notice about this work is not given;

161 Or, rather, every time the automated processes embedded in the software are programmed to interact with the software on my machine.

162 There are still other potential legitimate purposes for circumvention: see chapters 4, 5, and 7.

3) the data subject is not provided with the capability to prevent the information from being gathered or disseminated;
4) circumvention of the controls has the sole effect, and is solely for the purpose, of preventing the collection or dissemination; and
5) circumvention does not breach another law.[163]

The above provisions are narrow and, given the number of conditions that must be satisfied before the exception applies, the privacy protection that they afford is more apparent than real. Still, there is value in having an explicit provision permitting anti-circumvention for the purposes of protecting personal information. Canada's proposed anti-circumvention laws offer nothing. One might anticipate arguments that Bill C-60 needs no such provision because a circumvention for personal information protection purposes would not be illegal, since the Bill only applies to circumvention for an "infringing purpose." I do not find this argument to be compelling. Clarity and precision are crucial. Statutory silence on this issue will only provide fuel for unnecessary litigation campaigns by the copyright industries and other powerful stakeholders.

In the section that follows, I will try to "break the silence" by modestly articulating a summary account of three recommendations that would provide the kinds of counter-measures necessary to offset the new powers and protections afforded to TPM and DRM if Canada's anti-circumvention laws are implemented as proposed.

## G. SUMMARY OF RECOMMENDATIONS

### 1) An Express Provision Prohibiting the Circumvention of Privacy by TPM/DRM, Notwithstanding Licence Provisions to the Contrary

An appropriate counter-measure could be achieved by transposing the proposed anti-circumvention law into the privacy context. This would generate a kind of "anti-circumvention" provision which prohibits the use of TPM/

163 Above note 2. The above summary belongs to Lee Bygrave: Bygrave, above note 28 at 440. Bygrave also considers (in the European context) whether and when an end-user can take steps to prevent the operations of TPMs, and whether the concept of a technical measure extends to "devices that monitor usage." He concludes that monitoring devices which are incidentally concerned with [the prevention/restriction of unauthorized copying] fail to qualify as technical measures and therefore are not subject to anti-circumvention laws.

DRM to collect, use, or disclose personal information (or otherwise monitor identifiable individuals) in contravention of existing privacy law. In order for this counter-measure to be effective, it is crucial for the law to expressly provide that privacy-waivers or other similar contractual provisions built into the standard forms of DRM licenses shall not be enforceable where the collection, use, or disclosure by the DRM would otherwise contravene Canadian privacy law or other pressing public policy considerations.[164] Likewise, the counter-measure will only be effective if appropriate penalties or remedies for the circumvention of privacy laws are provided.[165]

---

164 The express provision recommended here is in part necessary because Canadian courts so often express deference to the legislature when rendering decisions about the scope of the court's power to deem a contract illegal or void public policy: *Richardson v. Mellish*, [1824] 130 E.R. 294 at 303; *Janson vs. Driefontein Consolidated Gold Mines, Ltd.*, [1902] A.C. 484 at para. 4; *Prarie Roadbuilders Ltd. v. Stettler (County No. 23)*, [1983] A.J. No. 774 at para. 39; *L.E. Shaw Ltd. v. Berube-Madawaska Contractors Ltd.*, [1982] 138 D.L.R. (3d) 364; Richard H.W. Maloy, "Public Policy: Who Should Make It in America's Oligarchy?" (1998) Det. C.L. Rev. 1143. An express provision of this sort is justified by virtue of Parliament's express desire to preclude organizations from tying the consent to purchase a product or services to a secondary consent to collect, use, or disclose personal information, set out in *PIPEDA*, above note 19, Principle 4.3.3. When DRM uses the device of contract to achieve this end, it contravenes *PIPEDA* and thereby provides ample justification for deeming any privacy waivers or other similar contractual provisions to be unenforceable or, to use the language of the common law, "void or public policy."

165 As discussed above at note 48, the Privacy Commissioner cannot order damage awards [See, Canada, Privacy Commissioner of Canada, *Annual Report to Parliament 2003-2004* (November 2004), <www.privcom.gc.ca/information/ar/200304/200304_e.asp>, at 58; Canada, Privacy Commissioner of Canada, *Annual Report to Parliament 2002-2003* (September 2003), <www.privcom.gc.ca/information/ar/02_04_11_e.asp>, at 57; Canada, Privacy Commissioner of Canada, *Annual Report to Parliament* 2001-2002 (January 2003), <www.privcom.gc.ca/information/ar/02_04_10_e.asp>, at 59. As noted on the Privacy Commissioner's site, summaries are not posted for all findings, <www.privcom.gc.ca/cf-dc/index_e.asp>] . Of the 542 cases that the Privacy Commissioner has investigated, only six cases have been commented on by the Federal Court [*Blood Tribe Department of Health v. Privacy Commissioner of Canada,* 2005 FC 328; *Diane L'Écuyer v. Aéroports de Montréal and Privacy Commissioner of Canada,* 2004 FCA 237; *Erwin Eastmond v. Canadian Pacific Railway and Privacy Commissioner of Canada,* 2004 FC 852; *Janice Morgan v. Alta Flights (Charters) Inc.,* 2005 FC 421; *Mathew Englander v. Telus Communications Inc. and Privacy Commissioner of Canada,* 2004 FCA 387; *Ronald G. Maheu v. IMS Health Canada et al.,* 2003 FCA 462]. Not a single one of these cases has attracted a damage award. Two of the complainants were able to recoup their costs: Mathew Englander and Ronald G. Maheu. Three cases saw the

### 2) An Express Provision Stipulating that a DRM Licence is Voidable when it Violates Privacy Law

In addition to the first recommendation, which ensures that DRM cannot be used to undermine statutory privacy protections without appropriate penalties/remedies, a broader contractual remedy is needed for individuals whose privacy has been breached. Individuals should not be forced to continue the contractual relationship in such circumstances. They should have the option to avoid such contracts, treating any obligations set out in the licence as at an end.

### 3) An Express Provision Permitting the Circumvention of TPM/DRM for Personal Information Protection Purposes

A third counter-measure needed to achieve an appropriate balance is a provision that helps to draw a laser-bright line between "infringing" and other purposes for circumventing a TPM/DRM. In particular, the provision must expressly permit the circumvention of technological measures where necessary for personal information protection purposes, stating its scope and limits. This would certainly include circumstances in which the DRM is operating in breach of privacy laws, but should also include circumstances where an individual needs to circumvent a technological protection measure in order to confirm the possibility of such a breach. While some might not perceive "mere suspicion" to be a sufficient reason to circumvent a DRM, privacy law currently affords similar powers to DRM to collect, use, or disclose personal information without knowledge and consent in order to ensure an organization's security and for other related purposes.[166] To achieve balanced legislation, it is suggested that the scope of permission afforded to individuals to circumvent TPM/DRM should generally be proportional to the scope of permission afforded to

---

court awarding no costs to either party. In one case, the complainant had to bear his as well as his opponent's legal costs: Erwin Eastmond.

166 See especially, *PIPEDA,* above note 19, s. 7(1)(b). At the same time, limits must surely be placed on a large and liberal interpretation of the section 7 exceptions since they might otherwise be used to justify ubiquitous 24/7 surreptitious surveillance on the grounds that any user might potentially violate any contractual agreement at any time. At the end of the day, these exemptions, like collection, use, and disclosure itself, must be limited by the "reasonableness" standard.

organizations to circumvent the knowledge and consent requirements of privacy law under analogous circumstances.[167]

## H. CONCLUSION

Canada's copyright reform process has been slow and deliberate. It has been consultative and inclusive. It canvasses a broad array of issues for reform. In its decision to tie the act of circumvention to "infringing purposes," the Government of Canada has demonstrated some willingness to approach the "appropriate balance" it purportedly strives towards.

Not so when it comes to privacy. Despite the obvious privacy threats that automation, cryptographic techniques, and other DRM technologies impose, the proposed anti-circumvention laws protect these technologies without protecting people from excessive or illegitimate uses of them.

Counter-measures are needed. If our laws are to prohibit people from circumventing the technologies that protect copyright, then they ought also to prohibit those same technologies from circumventing the laws that protect privacy. If the Government wishes to extend its copyright laws to regulate copyright enforcement technologies, then it must include rules that place restrictions upon the private powers that those technologies are now able to exert. If digital and network technologies increase the prospect of digital piracy, then our proposed solutions ought not to diminish the prospect of digital privacy. The legitimate goal of online anti-piracy protection must not succumb to the excessive and dangerous business of online anti-privacy protection.[168]

---

167 See s. 7, *ibid.*

168 One begins to believe in Freud when one re-reads the headnote and para. 17 of the official Federal Court decision in *BMG Canada Inc. v. John Doe*, [2004] 3 F.C.R. 241, 2004 FC 488, <http://reports.fja.gc.ca/fc/2004/pub/v3/2004fc34396.htm>, which (in)advertently characterizes MediaSentry (a business "enabling the successful growth of online distribution for companies in the entertainment and software industries" <www.mediasentry.com/corp/overview/index.html>) as an "online anti-privacy protection business." I owe the enjoyment of reporting this delicious irony to my brilliant, witty colleague, Jane Bailey, who first spotted this and shared it with me.