CANADIAN PRIVACY LAW REVIEW
FORTHCOMING 2005

HACKING @ PRIVACY: ANTI-CIRCUMVENTION LAWS, DRM AND THE PIRACY OF PERSONAL INFORMATION

Ian Kerr*

A. INTRODUCTION

Feeling the heat from the US and other countries that have long since ratified the *WIPO Copyright Treaty*,[1] this past summer, after much consultation and consternation, Canada proposed legislation that would prohibit the circumvention of technological measures designed to protect copyright. Introduced in Bill C-60,[2] its so-called *anti-circumvention* provision offers remedies against anyone who: "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…"[3] According to its drafters, a central aim of the proposed legislation 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."[4]

It is my contention 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 technological protection measures (TPMs) and the Digital Rights Management Systems (DRMs) that they support to engage in excessive monitoring, or the piracy of personal information. Copyright holders should not be permitted to use

* Canada Research Chair in Ethics, Law & Technology, Faculty of Law, University of Ottawa (*iankerr@uottawa.ca*). This article is an adaptation of "If Left to Their Own Devices: How DRM and Anti-Circumvention Laws Can Be Used to Hack Privacy" in M. Geist, *In The Public Interest: Canadian Copyright in a Digital Age* (Toronto: Irwin Law, 2005) <http://209.171.61.222/PublicInterest/Two_03_Kerr.pdf>. 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 that Chapter derives. Special thanks also to Dr. Hilary Young for her lead role in the adaptation of this article, and for her extraordinary efforts, her brilliance, and for the high quality of research assistance that she so regularly and reliably provides.

[1] *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>.

[2] 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>.

[3] *Copyright Amendment,* above note 2, s. 3 .02.

[4] *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>.

DRMs to circumvent fair information principles or to hack privacy legislation. In this brief paper, I explain why this is so and offer a general description of the kind of countermeasures that are needed to ensure that Canada's anti-circumvention provision adequately balances different stakeholder interests.

B. TPM/DRM

Before examining the policy implications of Bill C-60, it is useful to distinguish between TPMs and DRMs. In its simplest form, a TPM is a technological measure intended to promote the authorized use of digital works. Of course, TPMs can also operate as a kind of "virtual fence" around digitized content and can lock it up - whether or not it enjoys copyright protection. Both are accomplished by controlling access to such works, or by controlling various uses of such works, including: (i) copying, (ii) distribution, (iii) performance, and iv) display.

While TPMs are designed to *prevent* copying, DRMs are designed to *manage* copying, using various automation and surveillance technologies to identify content and technologically enforce certain licensing conditions. More and more, DRMs will be used to "manage" all rights reserved by content owners/providers – usually on a take-it-or-leave-it basis. Typically, a DRM consists of two components.

The *first component* is a set of technologies that might include: encryption, authentication, access control, digital watermarking, tamper-resistant hard and software and risk management architectures. Such 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. Usually, the ongoing exchange of personal information between users' devices and content owners'/providers' servers takes place in an invisible handshake occurring in the software layer. This allows the transmission of personal usage information back to the content owner/provider - something Greenleaf once cleverly described as "*IP phone home.*"[5]

Other technologies are used to *express* copyright permissions in "rights expression languages" and other forms of metadata that make a DRM policy machine-readable. 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.

[5] 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 21 [Bygrave, "Digital Rights Management and Privacy"].

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. The information that is collected can be employed in a number of 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 one's ability to subsequently distribute it to others who have not.

The surveillance features associated with the database are crucial to the technological enforcement 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.

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. DRM has the ability to monitor an individual's private activities while browsing, sampling, or shopping. But it can also be used to collect information or monitor behaviour after a contract is entered into, with the aim of scrutinizing a user's habits and activities 24/7, including (but certainly not limited to) whether the user has complied with the contract.

It should therefore be evident that a full-blown DRM is much more than just a "virtual lock", yet surprisingly, 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 and, worldwide, is surprisingly sparse.

Since the purpose of the proposed anti-circumvention provisions is to facilitate the implementation of DRM as a primary means of enforcing digital copyright, it should be clear 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."[6]

With an increasing reliance on automation and wireless technologies, these monitoring systems are becoming our more constant companions. The key difference is that *these* companions are seeking to monitor not what is going on *in our homes*, but rather, what is going on *in our heads*. This is a dangerous practice to allow, let alone protect (as Bill C-60 would do), especially considering that many of the corporations building these mechanisms of social control into the content delivery system are also attempting to corner the production market, embedding corporate imperatives into the content itself. When this happens, the erosion of public spaces for debate and thoughtful exchange disappear because the roadway *and* the scenery are artificially controlled.

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

Given DRM's surveillance capability, 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. Below, I briefly discuss three policy considerations that are crucial in achieving an appropriate balance between DRM and privacy: (i) the Anonymity Principle; (ii) Individual Access; and (iii) DRM Licenses. These will form the basis for three recommendations that I offer in response to Canada's proposed anti-circumvention laws.

1) The Anonymity Principle

There is no doubt that the ability to disconnect one's identity from one's actions is of tremendous instrumental and social value. It allows for intellectual development, for example by allowing people to assume roles and thereby test the plasticity of their identities and the social norms from which they are constituted. In addition, anonymity facilitates the flow of information on public issues and lends a voice to speakers who might otherwise be silenced by fear of retribution.

Anonymity also plays an important role in privacy. It can enhance privacy by: making it more difficult for others to control the collection, use, and disclosure of one's personal information; by protecting people from unwanted intrusions; and by focusing attention on "the content of a

[6] 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 101.

message or behavior rather than to the nominal characteristics of the messenger."[7]

Nevertheless, the social utility of anonymity has limits. As Lawrence Lessig once noted, "[p]erfect anonymity makes perfect crime possible."[8] On the Internet, however, the prospect of true anonymity is largely illusory: the Internet presents an imperfect blend of anonymity and identifiability.[9] This is perhaps as it should be, but as the previous section illustrated, that blend of anonymity and identifiability could substantially change with DRM thrown into the mix.

Recall that various 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 who is reading what.[10] 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 confuse how something is with how it must necessarily be.[11] If, as Weinberg suggests, the purpose of DRM is to ensure that "a packet stream requesting access comes from a person who has paid or is otherwise entitled to access"[12], then DRM *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, etc.

---

[7] 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).

[8] Lawrence Lessig, "The Path of Cyberlaw" (1995) 10 Yale L.J. 17 3 at 1750. See also A. Michael Froomkin, *Anonymity and Its Enmities* (June 1995) J. Online L. Art. , <www.wm.edu/law/publications/jol/95_96/froomkin.html>, at para. 6.

[9] 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"].

[10] 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 17.

[11] Lawrence Lessig, *Code and Other Laws of Cyberspace* (New York: Basic Books, 1999) at 2 –29 [Lessig, "Code and Other Laws"].

[12] Weinberg, above note 9 at 1279.

Not only is it technologically possible to implement DRM while maintaining the anonymity principle, but to do so is required by many states' privacy laws. In Canada, for example, 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".[13] Since many of the current identification and surveillance features of DRM generally are not necessary, 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.[14]

Infusing the anonymity principle into the design of DRM is certainly to be promoted as a matter of public policy, but it is crucial to recognize that it is by no means sufficient to protect privacy. Given the market failures of privacy-enhancing technologies to date, 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 DRMs designed to circumvent the anonymity principle where there is no justification for doing so.

2) Individual Access

In the copyright context, 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. 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. 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*. This might entail a positive obligation to allow access-to-works in the public domain, or to provide unfettered access-to-works to organizations, such as universities, that are currently exempted from a number of the provisions in the *Copyright Act.*

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.[15] Informational privacy is premised on

[13] *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*], s. 5(3).

[14] Bygrave cites *DPD*, Art. 6(1)(e) and (c), together with Articles 7-8: Bygrave, above note 5 at 29.

[15] Schedule 1 of *PIPEDA*, above note 13.

the idea that individuals ought to be able to determine for themselves when, how, and to what extent information about them is communicated. 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, and subsequently to provide an individual with access to personal information which has been collected about him or her. Like digital content, personal information 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 facilitate the circumvention Canadian privacy law through DRM.

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

3) DRM Licences

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, intelligent agent technologies facilitate the automatic "negotiation" of contractual licences between content providers and users.

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 therefore exacerbates an already problematic inequality in the bargaining power between the licencors and licencees resulting from standard form agreements and mass market licenses. The combination of TPMs and contracts in this manner could therefore lead to unfair transactions.

With increasing frequency, the terms of these licences are used to override existing copyright limitations. And, as Guibault aptly articulates:

> 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.[16]

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. Like copyright, privacy law's compromise between the needs of organizations and the right of privacy of individuals 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.

There is therefore value in contemplating basic common law principles and their applicability for setting appropriate limits on DRM's ability to exploit the law of contract. As any first year law student will attest, contract law commences with the idea of freedom to contract — and then systematically proceeds to undermine the idea through various doctrines. 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."[17] While the courts generally avoid interfering with individual bargains, they will sometimes render void a contract that contravenes a statute.

To date, the Commissioner has issued no findings as to whether DRM surveillance contravenes *PIPEDA* or its provincial equivalents. 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 certainly have concerns about any commercial enterprise in Canada that deployed privacy-invasive DRM

---

[16] 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 160.

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

> technologies in contravention of the provisions of the *Personal Information Protection and Electronic Documents Act* (*PIPEDA*) and the fair information practices underlying it.[18]

This passage, though not intended as dispositive, lends credence to the possibility that a DRM device engaging in excessive monitoring or collection would contravene *PIPEDA*. 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."[19]

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."[20]

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,"[21] then the amendments to the *Copyright Act* must include a different set of anti-circumvention provisions. We need counter-measures that expressly prohibit the use of DRM to circumvent the protection of Canadian privacy law. "Appropriate balance" requires a legal lock aimed at organizations that would use TPMs, the proposed anti-circumvention law, and the law of contract as a means of hacking at *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.

When it comes to DRM and privacy, there are two kinds of consent. The first is the consent required to give rise to the DRM contractual licence. The second is the consent required to satisfy FIPs. FIPs consent is usually

---

[18] Letter to Phillipa Lawson and Alex Cameron from Privacy Commissioner of Canada, (2 November 200), <www.cippic.ca/en/projects-cases/copyright-lawreform/LF%20Privacy%20Commissioner%20re%20copyright%20and%20DRM%20&%20TPM%20-%20Nove%202 %200 .pdf> [Letter]. I am indebted to Alex Cameron for alerting me to the existence of this letter.

[19] Jennifer Stoddart, Letter, above note 18. 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."

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

[21] *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/rp011 3e.html>.

a much more robust form of statutory consent. It is crucial to note the distinction. As Daniel Solove notes:

> 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.[22]

Thus, the legal threshold for contractual consent is not well-suited to protecting privacy. If such protections were within the exclusive domain of contract law then there would be practically none. In too many instances, "freedom of contract" means "take-it-or-leave-it." So too, DRM licences, *if left to their own devices*, will offer all or nothing contracts: "either consumers agree to forgo privacy, or else they forgo access."[23] In some instances, and privacy is certainly one of them, what people need is freedom *from* contract.

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

1) Appropriate Purpose

Section 5(3) of *PIPEDA* uses the common law construct of the "reasonable person" to limit 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.[24]

Thus, even if a person carefully considers and then expressly consents to the collection of personal information, her consent will not justify collection if the purpose for collection is said to be unreasonable. 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

---

[22] Daniel J. Solove, *The Digital Person: Technology and Privacy in the Information Age* (New York: NYU Press, 200) at 82–85.

[23] I borrow this way of characterizing things from Ann Bartow.

[24] *PIPEDA,* above note 13, s. 5(3).

bargaining process, the courts are loath to determine whether the bargain between the parties is reasonable. Not so with the application of this section of the legislation. 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 above, Principle 4.3 of Schedule 1 in *PIPEDA* 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 usually not simply be deemed to consent but must rather be said to consent *knowingly*.

A further provision ensures 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.

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. "Sensitive" information will generally require more detailed and in some instances express consent. The rationale for this is that "in obtaining consent, the reasonable expectations of the individual are also relevant."[25] Note that this is a different "reasonableness" requirement than the one discussed in the preceding section. There, the reasonableness related to an organization's purposes for collection, use, or disclosure. Here, reasonableness relates to the information subject's actions and whether consent can truly be inferred from them. One further difference between contractual consent and the consent requirement in *PIPEDA* is that only in the latter can consent be withdrawn with impunity. 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.

Even this brief snapshot should illustrate that the concept and application of consent in Canadian privacy law is nuanced and difficult. 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,

[25] *Ibid.*, Sch. 1, cl. .3.5.

nor to data-mine or conduct surveillance against those who use DRM-delivered intellectual content.

This point was not overlooked by those who enacted Canada's privacy legislation. *PIPEDA* contains a "refusal to deal" clause, which highlights the need to distinguish between DRM's contractual consent and a significantly higher threshold in FIPs consent. Principle 3.3 prohibits an organization from requiring an individual to consent to the collection, use, or disclosure of information as a condition of the supply of a product or service.This provision is a clear limitation on the take-it-or-leave-it approach of DRM's contractual consent.

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 in a manner that permits and protects privacy-invasive 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, compel the courts to enforce and give effect to their illegal transaction."[26] Privacy law is meant, in some instances, to provide *freedom from contract*.

F. THE SOUNDS OF SILENCE

Having examined 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. 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.[27] The effect of these paracopyright provisions will be to further expand the law of copyright so that it includes certain *acts* that have nothing to do with copying, such as: "circumvent[ing], remov[ing] or in any way render[ing] ineffective a technological measure protecting any material form of the work" and "knowingly remov[ing] or

[26] Ritchie C.J, above note 20.

[27] See ss. 34.01 and 34.02 of *Copyright Amendment*, above note 2.

alter[ing] any rights management information in electronic form that is attached to or embodied in any material form of the work."[28]

By treating the circumvention of a TPM as a copyright infringement, 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,"[29] which will have a chilling effect on important research in cryptography and other areas.

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 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, as well as the need for "openness" in organizations about the policies and practices relating to their management of others' personal information. 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, one might wish to tinker with a DRM — not to interfere with its copyright enforcement function but in the interest of knowing whether excessive collection or monitoring is taking place. Perhaps one even suspects this, in which case the purpose of circumvention is to achieve transparency. 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? 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

[28] *Ibid.*, s. 34.02.

[29] See for example, Edward W. Felten, "Freedom to Tinker," <www.freedom-totinker.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>.

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.

One might anticipate arguments that Bill C-60 needs no such provision because circumvention for personal information protection purposes would not be illegal, since the Bill only applies to circumvention for an "infringing purpose." This argument is not compelling. Statutory silence on this issue will only provide fuel for unnecessary litigation campaigns by the copyright industries and other powerful stakeholders.

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

G. SUMMARY OF RECOMMENDATIONS

1) Include 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/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, the law must 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. Likewise, the counter-measure will only be effective if appropriate penalties or remedies for the circumvention of privacy laws are provided.

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

In addition to the first recommendation, a broader contractual remedy is needed for individuals whose privacy has been breached. Individuals should have the option to avoid such contracts, treating any obligations set out in the licence as at an end.

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

A third counter-measure would 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. To achieve balanced legislation, it is suggested that the scope of permission afforded to individuals to circumvent TPM/DRM should be proportional to the scope of permission afforded to organizations to circumvent the knowledge and consent requirements of privacy law under analogous circumstances.

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 surveillance 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.