

**Submission to
The House of Commons Standing Committee on
Access to Information, Privacy and Ethics**

on

***The Personal Information Protection and
Electronic Documents Act (“PIPEDA”) ¹***

Appearance Date: Monday, December 11, 2006

Dr. Ian R. Kerr

Canada Research Chair in Ethics, Law & Technology
Faculty of Law, University of Ottawa
57 Louis Pasteur St., P.O. Box 450, Stn.A
Ottawa, Ontario K1N 6N5
tel: 613.562.5800 ext. 3281
fax: 613.562.5124
iankerr@uottawa.ca
iankerr.ca
idtrail.org

¹ The author expresses his most sincere gratitude to Anne Uteck, Dr. Hilary Young, Katie Black and Felix Tang for their valuable assistance in the preparation of these submissions.

Biography

Ian R. Kerr

B.Sc. (Alberta), B.A. (Hons.) (Alberta), M.A. (U.W.O.), LL.B. (U.W.O), Ph.D. (Philosophy of Law) (U.W.O), of the Bar of Ontario, Associate Professor, Canada Research Chair in Ethics, Law & Technology.

Ian Kerr holds a unique, three way appointment in the Faculty of Law, the Faculty of Medicine and the Department of Philosophy at the University of Ottawa. His devotion to interdisciplinary teaching has earned six awards and citations, including the Bank of Nova Scotia *Award of Excellence in Undergraduate Teaching*, the University of Western Ontario's Faculty of Graduate Studies' *Award of Teaching Excellence*, and the University of Ottawa's AEECLSS *Teaching Excellence Award*. Professor Kerr currently teaches a graduate seminar in the LLM concentration in law and technology (*Technoprudence: Legal Theory in an Information Age*), as well as a unique seminar offered each year during the month of January in Puerto Rico that brings students from very different legal traditions together to exchange culture, values, and ideas and to unite in the study of privacy and other technology law issues of global importance. Professor Kerr also teaches in the areas of moral philosophy and applied ethics, internet and ecommerce law, contract law and legal theory.

In 2001, Professor Kerr was awarded the *Canada Research Chair in Ethics, Law and Technology*. He is one of Canada's leading privacy scholars and has also published writings in academic books and journals on ethical and legal aspects of digital copyright, automated electronic commerce, artificial intelligence, cybercrime, nanotechnology, internet regulation, ISP and intermediary liability, online defamation, pre-natal injuries and unwanted pregnancies.

His current program of research includes directing two large projects: (i) *On the Identity Trail*, a four year, four million dollar project involving more than 50 researchers from across North America, supported by one of the largest ever grants from the Social Sciences and Humanities Research Council. This project focuses on the impact of information and authentication technologies on our identity and our right to be anonymous; and (ii) *An Examination of Digital Copyright*, supported by half million dollar private sector grant from Bell Canada and the Ontario Research Network in Electronic Commerce, focusing on various aspects of the current effort to reform Canadian copyright legislation, including the implications of such reform on fundamental Canadian values including privacy and freedom of expression.

In addition to the management of these large projects, he also co-directs the *Canada Research Chair Laboratory in Law and Technology*, a facility that supports the work of more than 40 researchers. He is a member of the Law Society of Upper Canada, the Academic Coordinating Committee of the Centre for Innovation Law and Policy, the Centre for Ethics and Values, the Canadian Association of Law Teachers, the Canadian Bar Association, and the Uniform Law Commission of Canada's Special Working Group on Electronic Commerce. He is an associate editor of Kluwer's *Electronic Commerce Research Journal*, a guest editor for *Presence: Teleoperators and Virtual Environments* (MIT Press), and sits as a member on the Advisory Board of the Canadian Internet Policy and Public Interest Clinic and on the Advisory Board of Butterworths' *Canadian Internet and E-Commerce Law Newsletter*. He is also co-author of *Managing the Law: The Legal Aspects of Doing Business* (Prentice Hall), a business law text used by thousands of students each year at universities across Canada.

Summary

PIPEDA is a consent-based model of personal information protection. As our current Privacy Commissioner recently put it, consent is “the fundamental principle on which PIPEDA is based”. Consent is the legal mechanism through which individuals exercise their rights pursuant to PIPEDA to determine for themselves when, how and to what extent information about themselves is communicated to others. Consent is therefore the gatekeeper of unwanted collection, use or disclosure of personal information.

This two part submission focuses on the immediate need to revise the consent provisions in PIPEDA.

The first part summarizes the main problems of consent within the existing provisions of PIPEDA and recommends various specific revisions to remedy its current vagueness, alleviate confusion about the application and enforcement of the law, and increase business certainty:

- increase notice requirements
- amend ‘refusal to deal’ clause
- redraft consent provisions to distinguish between express, implied, and deemed/opt-out consent and to establish clear criteria for each
- require that personal information generally be collected directly from the individual and specify the consent gathering process for indirect collection
- tighten other specified consent requirements

The second part of this submission introduces a novel set of privacy concerns arising when organizations exploit the law of contract to evade their privacy obligations pursuant to PIPEDA. Drawing on foundational common law principles, it provides a series of recommendations to prevent contract law from undermining PIPEDA’s personal information protection provisions:

- stipulate that the existence of a contract claiming to permit personal information collection has no evidentiary relevance to a determination of the purported reasonableness or appropriateness of its collection, use and disclosure practices
- stipulate a series of conditions under which contracts requiring an individual to contract out of privacy protections provided for in PIPEDA shall not be enforceable
- stipulate that organizations may not prohibit an individual from withdrawing consent to the collection, use or disclosure of personal information related to the individual
- provides the Privacy Commissioner (or an associated Tribunal) with order-making powers, including the power to award damages

Introduction

This two part submission focuses exclusively on the immediate need to revise the consent provisions in PIPEDA.

The first part summarizes the main problems of consent within the existing provisions of PIPEDA and recommends various revisions to remedy its current vagueness, alleviate confusion about the application and enforcement of the law, and increase business certainty. The second part of this submission introduces a novel set of privacy concerns arising when organizations exploit the law of contract to evade their privacy obligations pursuant to PIPEDA. Drawing on foundational common law principles, it provides a series of recommendations to prevent contract law from undermining PIPEDA's personal information protection provisions.

I. Consent within PIPEDA

PIPEDA is a consent-based model of personal information protection. As our current Privacy Commissioner recently put it, consent is "the fundamental principle on which PIPEDA is based".² Consent is the legal mechanism through which individuals exercise their rights pursuant to PIPEDA to determine for themselves when, how and to what extent information about themselves is communicated to others.³ Consent is therefore the gatekeeper of unwanted collection, use or disclosure of personal information.

In accord with previous testimony collected during this legislative review process,⁴ it is submitted that the current consent requirements set out in PIPEDA are vague and uncertain, thereby diminishing individuals' ability to control the collection, use and disclosure of personal information while, simultaneously, increasing expenditures of time and money by businesses that aim to comply with the law. The following paragraphs offer a summary of the main consent problems within PIPEDA and are accompanied by five specific recommendations for revision.

PIPEDA generally requires 'knowledge and consent'⁵ as a legal prerequisite to the collection, use, and disclosure of personal information. However, the notion of consent is not defined in the Act. The result has been a wide and unwieldy set of

² Jennifer Stoddart, "An Overview of Canada's New Private Sector Privacy Law – The Personal Information Protection and Electronic Documents Act", online: <http://www.privcom.gc.ca/speech/2004/vs/vs_sp-d_040331_e.asp>.

³ Alan Westin, *Privacy and Freedom* (New York: Athenum, 1970).

⁴ See submissions by Colin Bennett (online: <<http://www.cippic.ca/en/projects-cases/privacy/submissions/ColinBennett2006PIPEDASubmission.pdf>>) and CIPPIC (online: <http://www.cippic.ca/en/projects-cases/privacy/submissions/CIPPIC_Submission_Nov06wFNs.pdf>). See also Michael Geist's Toronto Star column on this issue (online: <http://www.thestar.com/NASApp/cs/ContentServer?pagename=thestar/Layout/Article_Type1&c=Article&cid=1163976613842&call_pageid=968350072197>).

⁵ *Personal Information Protection and Electronic Documents Act* S.C. 2000, c.5 [*PIPEDA*], Schedule 1, s. 4.3. Note: 'knowledge and consent' is sometimes referred to as 'informed consent'.

incommensurate interpretations and inconsistent business practices across the marketplace.⁶

Principle 4.3.4 allows for the form of consent sought by an organization to vary, but PIPEDA does not distinguish between express, implied, and deemed/opt-out consent. It provides no criteria or conditions as indicia of when an organization can and cannot rely on a particular form of consent. Further, many of the so-called 'consent' gathering processes used by organizations today *do not* result in genuine knowledge and consent. For example, many organizations use a personal information collection tactic that separates an opt-out mechanism from the initial consent process in a way that places an undue burden on individuals to withdraw consent that those individuals never actually provided in the first place. This not only increases the likelihood that consent is falsely presumed from the outset, it also preys on well known psychological barriers to withdrawing consent: people who are required to actively opt-out are psychologically predisposed against doing so, even if there are good reasons in favour of doing so.⁷

Additionally, particular confusion stems from the use of the term 'implied consent.' While the Privacy Commissioner has published guidelines for determining the appropriate form of consent,⁸ recent survey findings demonstrate that this is not sufficient: many organizations lack an understanding of the need for informed consent, the differences between opt-in and opt-out consent, and the appropriate limits on using opt-out methods achieving valid consent.⁹ Survey results also show that a large number of organizations do not obtain meaningful consent to secondary uses and disclosures of personal information. 'Blanket consent' clauses are used to provide organizations with *the appearance* of broad and unspecified permissions to use and disclose information. However, since no such permission was ever given (and, if asked, individuals will often refuse such permission), such practices render the consent principle meaningless.

Likewise, notice requirements are covered under Principle 4.3.2. but, as with consent, PIPEDA does not specify any clear or practicable criteria for notice. Without ensuring adequate notice, 'knowledge and consent' are unachievable.

Recent private sector privacy legislation in both the British Columbia and Alberta have responded to many of the problems set out above, significantly improving the clarity and precision of the consent requirements under their personal information privacy protection legislation.¹⁰

⁶ Canadian Internet Policy and Public Interest Clinic (CIPPIC), "Compliance with Canadian Data Protection Laws: Are retailers measuring up?" (Ottawa: CIPPIC, 2006) online: <[http://www.cippic.ca/en/bulletin/compliance_report_06-07-06_\(color\)_\(cover-english\).pdf](http://www.cippic.ca/en/bulletin/compliance_report_06-07-06_(color)_(cover-english).pdf)>.

⁷ Jennifer Barrigar, Jacqueline Burkell and Ian Kerr, "Let's Not Get Psyched Out of Privacy: Reflections on Withdrawing Consent to the Collection, Use and Disclosure of Personal Information" Canadian Business Law Journal (forthcoming).

⁸ Privacy Commissioner of Canada, "Determining the appropriate form of consent under the *Personal Information Protection and Electronic Documents Act*" (Ottawa: Privacy Commissioner of Canada, 2004) online: <http://www.privcom.gc.ca/fs-fi/02_05_d_24_e.asp>.

⁹ *Supra* note 6.

¹⁰ *Personal Information Protection Act* S.B.C. 2003, c.63 [BC PIPA]; *Personal Information Protection Act* S.A. 2003, c. P-6.5 [Alberta PIPA].

Given the extent to which vague standards and current business practices obfuscate the possibility of meaningful consent, the following recommendations are offered:

Recommendation #1

Require notification of specified information to the individual on or before collecting personal information (as in Alta PIPA s.13 and B.C. PIPA s.10).

Amend Principle 4.3.2, replacing "[o]rganizations shall make a reasonable effort to ensure that the individual is advised of the purposes for which the information will be used" with "organizations shall, on or before collecting personal information about an individual, disclose to the individual the purposes for which the information will be used."

Recommendation #2

Amend the poorly drafted 'refusal to deal' section in PIPEDA (Principle 4.3.3) by replacing "...beyond that required to fulfil the explicitly specified and legitimate purposes" with ".....beyond what is necessary to provide the product or service" (see subs.7(2) of Alta and BC PIPAs).

Recommendation #3

Redraft PIPEDA's consent provisions along the lines of the Alberta and B.C. legislation, so as to distinguish between express, implied, and deemed/opt-out consent and to establish clear criteria for each (see ss.7, 8 of Alta and BC PIPAs).

The provision regarding deemed/opt-out consent should require that notice be provided not only "in a form that the individual can be reasonably expected to understand" but also "in a manner that that individual can be reasonably expected to notice".

Recommendation #4

Include in Principle 4.4 of PIPEDA a requirement that personal information be collected directly from the individual unless the individual has consented to indirect collection, in which case the collecting organization should be required to give the disclosing organization sufficient information about the purposes for collection to allow the latter to ensure that the individual has consented to that use/disclosure (see Alta PIPA subs.7(1)(b) and 13(3)).

Recommendation #5

In Principle 4.3.1, replace the two last sentences: “[t]ypically, an organization will seek consent for the use or disclosure of the information at the time of collection...” with “except when seeking consent for a purpose not previously identified, organizations shall seek consent for the use and disclosure of the information at the time of collection. If relying upon opt-out consent, organizations shall give individuals the opportunity to opt-out before consent is assumed.”

II. Contracting-Out of PIPEDA

We live in an information age. The information trade, its services and its technologies of irresistible convenience demand *quid pro quo*: in order to *get* information products, you must *give up* some personal information. Computers and other information technologies pose new threats to privacy. Former Privacy Commissioner of Canada, Bruce Phillips, described PIPEDA as a response to these threats:

This statute ... constitutes the first determined effort to place a check upon, and ultimately to reverse, the massive erosion of individual privacy rights brought about by the application of computer and communications technology in the commercial world.¹¹

It is true that computers, databases, networks, surveillance cameras, cookies, spyware, radio frequency identification and other automated means of collecting, using and disclosing personal information directly threaten our ability to control personal information. It is submitted here, however, that the bigger threat to privacy is a legal threat: the standard form contract. While the above mentioned devices *technologically enable* aggressive, voluminous and sometimes surreptitious collection, use and disclosure of personal information, it is standard form contracts that *legally enable* the ‘implied’, ‘deemed’ and ‘opt-out’ consent-gathering processes said to justify the use of surveillance technologies under our current privacy law.

Standard form contracts are mass-produced documents that prevent and preclude negotiation and agreement. They are drafted exclusively by parties in an economic position to offer certain terms on a *take-it-or-leave-it* basis. In an information age, where the business handshake has been replaced by mouseclicks, where one-to-many transactions supplant bilateral negotiation, the standard form contract is regularly invoked by organizations to circumvent various privacy protections prescribed in PIPEDA.

Whether in the sale of goods or the licencing of services, many organizations use standard forms, clickwraps and end-user license agreements as a way to justify unreasonable and overarching ‘consent’ to excessive collection, use and disclosure of personal information, extending their personal information practices well beyond the bounds of what might otherwise be permitted by Canadian privacy law.

¹¹ Bruce Phillips, “Foreword” in Stephanie Perrin, Heather H. Black, David H. Flaherty and T. Murray Rankin, *The Personal Information Protection and Electronic Documents Act: An Annotated Guide* (Toronto: Irwin Law, 2001) at ix.

To offer an example, there are nearly 400,000 hotel rooms in Canada, many of which provide internet services for their many guests. Those that do, require customers to agree to various standard terms of use. Hilton hotels, for instance, required its customers to agree to the following:

"We may automatically track, collect and compile User Information and Transaction Data ... when you utilize the Service.

You agree that HHC shall own all Information.

By using the Service, you voluntarily, expressly and knowingly acknowledge and agree with all of the foregoing and further agree to each and all of the following: (i) such Information belongs to HHC and is not personal or private proprietary information; (ii) such Information, wherever collected, may be processed, used, reproduced, modified, adapted, translated, used to create derivative works, shared, published and distributed by HHC in its sole and absolute discretion in any media and manner irrevocably in perpetuity in any location throughout the universe without royalty or payment of any kind, without, however, any obligation by HHC to do so."¹²

It is submitted that PIPEDA's attempt to balance individual privacy rights with the need of organizations to collect personal information is undermined if, irrespective of PIPEDA's many protective provisions, intrusive, unfair or unwanted collection, use or disclosure can be imposed on individuals with impunity through standard form contracts such as those used by Hilton and other hotels, instant messaging services, mobile phone and other online service providers. By allowing organizations to require individuals to contract-out of obligations imposed by legislation, PIPEDA's purpose is completely undermined.¹³

Consequently, revisions to PIPEDA are needed to prevent organizations from using contract law to circumvent its prescribed obligations. To better understand why this is so, it is necessary to describe in further detail how organizations attempt to require individuals to contract-out of PIPEDA. This, in turn, requires an understanding of the differing legal thresholds for different kinds of consent. In particular, that contractual consent carries a much lower threshold than 'knowledge and consent' as required by PIPEDA and that the low threshold for contractual consent is therefore *not* a legal proxy for PIPEDA's consent requirements.

Contractual Consent versus PIPEDA Consent

Although PIPEDA generally requires 'knowledge and consent' for the collection, use and disclosure of personal information, as noted above, the notion of consent is not defined in the Act.

¹² "Hilton High-Speed Internet Service Agreement", online:
<<http://www.gripe2ed.com/scoop/story/2005/2/10/05746/7247>>.

¹³ PIPEDA s. 3.

In its broader common law context, consent is often characterized as “freely given agreement.”¹⁴ Because the “voluntary agreement” aspect is so central, consent is often linked to its corollary concept within the law of contract. However, in contract law, consent is understood as inherently transactional – a definable moment that occurs when the parties crystallize the terms and conditions upon which they agree. Contractual consent is determined at the moment the parties communicate their intention to be bound by that agreement.¹⁵ Once the parties have achieved a consensus, the contract is in place and the obligations become fixed. The moment this happens, the question of contractual consent is settled.

By contrast, the consent requirement set out in PIPEDA is not an isolated moment of agreement, but is conceived of as *ongoing* and can in fact be withdrawn at any time by the person about whom information is being collected. PIPEDA consent therefore has implications and effects that extend well beyond a specific transaction or series of transactions.

To understand and appreciate the *ongoing consent* doctrine, one must recall that PIPEDA is predicated on the notion that individuals have a *right* to control personal information about themselves. If individuals have such a right-of-control then, unless they surrender it, they retain ultimate control over their personal information in spite of consenting to its use by some organization. The consent afforded to an organization to use an individual's personal information must therefore be understood to be restricted. Consent *does not* give the organization ultimate control over personal information in perpetuity. In other words, the *continued use* of an individual's personal information must be understood as a necessary consequence, not of the initial consent to collect the information, but rather of that person's *continuing consent* to the organization to use that information. Consent, for the purposes of PIPEDA, must *not* be thought as an eternal release of information, nor as a complete assignment of control over the information. Rather, it is a license that permits only a *limited* collection, use or disclosure.¹⁶ Information *is not* unilaterally released when consent is given, but rather the individual maintains control over the ongoing management of her personal information.

Under PIPEDA there are at least three elements built into the legislation that demonstrate how the distinction between contractual and PIPEDA consent is crucial and, at the same time, why organizations would obviously prefer to invoke the lower threshold of contractual consent: (i) an appropriate purpose requirement; (ii) a higher statutory threshold for consent; (iii) a “refusal to deal” clause.

¹⁴ Daphne A. Dukelow and Betsy Nuse, *The Dictionary of Canadian Law*, 2nd ed. (Scarborough, On: Carswell, 1995) at 232.

¹⁵ See Gerald H. L. Fridman, *The Law of Contract in Canada*, 4th ed. (Scarborough, On: Carswell, 1999) at 16-17. See also Stephen Waddams, *The Law of Contracts*, 4th ed. (Toronto: Emond Montgomery Publications, 1999) at 66-67.

¹⁶ Under PIPEDA Principle 2 (s. 4.2.2 of Schedule 1), consent is only given for the purposes specified. Under Principle 4 (s. 4.4 of Schedule 1) these purposes must be appropriately limited, and under Principle 5 (s. 4.5 of Schedule 1) all uses or disclosures require consent and should be documented *per* s. 4.5.1. Almost any new purpose beyond those already specified requires new consent, as set out in s. 4.2.4.

(i) 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.¹⁷

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 the *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.¹⁸ 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.¹⁹ Not so with the application of this section of the legislation. Here the reasonableness of the purposes for collection, use, or disclosure is determinative.

Unfortunately, many organizations believe that they have satisfied the consent requirements simply by invoking a one-sided contract. Consequently, there is cause for concern that those organizations (and perhaps some courts) will conclude that such contracts also satisfied the reasonableness requirement in section 5(3) of PIPEDA. A statutory revision is therefore needed to clarify that the mere existence of a contract will not suffice.

Recommendation #6

Amend section 5(3) to include an additional paragraph stipulating that the existence of a contract claiming to permit personal information collection, has no evidentiary relevance to a determination of the purported reasonableness or appropriateness of its collection, use and disclosure practices.

(ii) Higher PIPEDA Threshold for Consent

PIPEDA sets higher thresholds for obtaining consent than would be afforded by way of contract law.²⁰ A number of the provisions of PIPEDA illustrate this higher threshold. Principle 4.3 of Schedule 1 requires knowledge and consent; the data

¹⁷ PIPEDA s. 5(3).

¹⁸ See for example Privacy Commissioner of Canada, "PIPED Act Case Summary #22: Company asks for customer's SIN as a matter of policy" (5 November 2001) online: <http://www.privcom.gc.ca/cf-dc/2001/cf-dc_011105_02_e.asp>. See also Nymity Inc., "Reasonable and the Reasonable Person within the Scope of PIPEDA" online: <http://www.nymity.com/faq/reasonable_and_the_reasonable_person.asp>.

¹⁹ *Miller v. Lavoie* (1966), 63 W.W.R. 359 at 365 (B.C.S.C.).

²⁰ Ian Kerr, "If Left To Their Own Devices: How DRM and Anti-Circumvention Laws Can Be Used to Hack Privacy" in Michael Geist (ed.), *In the Public Interest: The Future of Canadian Copyright Law* (Toronto: Irwin Law, 2005).

subject must be said to have *knowingly* consented to the collection, use or disclosure of personal information, except where inappropriate. This differs markedly from the law of contract where a party to a contract can be held to its terms even if it has neither read nor understood them.

A further PIPEDA requirement is that consent be “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.”²¹ PIPEDA also creates a higher threshold for consent by contemplating different forms of consent depending on the nature of the information and its sensitivity.²² Moreover, unlike the law of contracts, where consent is seen as a single transactional moment, PIPEDA allows the information subject to withdraw consent at anytime.²³ On the basis of these provisions, PIPEDA’s consent model is much more robust than the usual model for consent in contract law, which treats consent as an isolated moment of contractual agreement during an information exchange.

Generally, the threshold of consent is significantly higher in the privacy context than in contract law. The lower threshold of contractual consent is therefore too blunt a tool for privacy law and ought not to be used as a legal proxy. To do so would undermine the fair information practices upon which PIPEDA is founded. The legal threshold for contractual consent and the one-sided nature of standard form agreements is not a well-suited device for protecting privacy interests.²⁴ In fact, it is the entire reason why privacy legislation is necessary in the first place. If privacy protections were left to the exclusive domain of contract law – left entirely up-for-grabs in the bargaining process – then there would be no privacy protections. In too many instances, “freedom of contract” means “take-it-or-leave-it” where there is really no choice but to take-it, or be left behind.²⁵

(iii) ‘Refusal to Deal’ Clause²⁶

A third PIPEDA provision that highlights the need to distinguish between contractual consent and the higher threshold of PIPEDA consent is Principle 4.3.3, which states that:

²¹ PIPEDA Sch. 1 s. 4.3.2. Note, however, that there are limits on the high threshold of consent. See, for example, PIPEDA s.7(1)(b).

²² PIPEDA Sch. 1, s. 4.3.4.

²³ PIPEDA Sch. 1 s. 4.3.8. This section sets out that: “[a]n individual may withdraw consent at any time, subject to legal or contractual restrictions and reasonable notice. The organization shall inform the individual of the implications of such withdrawal.”

²⁴ See Daniel J. Solove, “Privacy and Power: Computer Databases and Metaphors for Information Privacy” (2001) 53 Stan. L. Rev. 1393; Paul M. Schwartz, “Privacy and Democracy in Cyberspace” (1999) 52 Vand. L.Rev. 1609, online: <<http://papers.ssrn.com/sol3/Delivery.cfm/000120306.pdf?abstractid=205449&mirid=1>>; Julie Cohen, “A Right to Read Anonymously: A Closer Look at ‘Copyright Management’ in Cyberspace” (1996) 28 Conn. L. Rev. 981; Julie Cohen, “DRM and Privacy” (2003) 18 Berkeley Tech. L.J. 575.

²⁵ Friedrich Kessler, “Contracts of Adhesion: Some Thoughts About Freedom of Contract” (1943) 43 Columbia L.R. 629 at 632.

²⁶ This clause was dubbed the ‘refusal to deal clause’ by the CSA Committee and was the subject of much debate. See Stephanie Perrin *et al.*, *supra* note 12 at 25.

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.

This provision is a clear and obvious limitation on the take-it-or-leave-it approach of contractual consent, and has been affirmed in several decisions. For example, 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.^{27 28} As some experts have described, "[t]he 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."²⁹

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. Contractual devices should not be permitted to circumvent these protections. Consumers, who often have no idea what is at stake, should be protected from organizations that try to use standard form agreements to contract-out of these privacy protections.

In response, basic common law principles are helpful in the development of two recommendations that would set appropriate limits on an organization's ability to exploit the law of contract in order to evade privacy obligations.

Limits on 'Freedom to Contract'

The law of contract still pays some homage to the doctrine of freedom to contract: the idea that it is up to the parties to determine their own bargains and that courts should be loath to interfere unless there is good reason to do so.³⁰ However, while courts generally tend to avoid interfering with individual bargains, they will refuse to enforce a contract in numerous situations. One such situation is where the contract is said to be illegal, i.e., when it: (i) contravenes a statute, or (ii) is inconsistent with public policy.

The federal Privacy Commissioner has given credence to the notion that digital rights management systems, end user licences and other contractual devices that circumvent consent requirements in order to engage in excessive collection of personal information contravene PIPEDA.³¹ There is also good reason to believe that courts will set aside a contract aiming to circumvent PIPEDA on the grounds of illegality. After all, as the Supreme Court of Canada ruled long ago, "[i]t would be a

²⁷ Privacy Commissioner, *supra* note 19.

²⁸ See Barbara McIsaac, Rick Shields, & Kris Klein, *The Law of Privacy in Canada*, (Toronto: Carswell, 2004) at 4-40.

²⁹ Perrin *et al.*, *supra* note 12 at 27.

³⁰ Waddams, *supra* note 16 at 399.

³¹ Letter to Phillipa Lawson and Alex Cameron from Privacy Commissioner of Canada, (24 November 2004), online: <www.cippic.ca/en/projects-cases/copyright-lawreform/LF%20Privacy%20Commissioner%20re%20copyright%20and%20DRM%20&%20TPM%20-%20Nove%2024%2004.pdf>.

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."³²

Even if a particular contract was not found to contravene PIPEDA – for example, if the information collected, used or disclosed did not require consent under the Act³³ – a court might find the terms of the contract unenforceable on the basis of public policy.³⁴ 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.³⁵ As such, a contract that permits excessive personal information collection, use or disclosure without 'knowledge and consent' as required by PIPEDA are likely unenforceable on public policy grounds, pursuant to the test for common law illegality.³⁶

In order to fulfill the Privacy Commissioner's claim that consent is "the fundamental principle on which PIPEDA is based,"³⁷ organizations must be required to meet PIPEDA's high threshold of consent and must not subvert these requirements through the device of contract. As such, further legislative reform is required to prohibit organizations from contracting out of PIPEDA's privacy obligations. The aim of such an amendment would be to render unenforceable the provisions in a contract that fail to respect PIPEDA's high threshold for consent.

³² *Bank of Toronto v. Perkins* (1893) 8 S.C.R. 603.

³³ PIPEDA Sch. 1 s.4.3 contains the following note:

In certain circumstances personal information can be collected, used, or disclosed without the knowledge and consent of the individual. For example, legal, medical, or security reasons may make it impossible or impractical to seek consent. When information is being collected for the detection and prevention of fraud or for law enforcement, seeking the consent of the individual might defeat the purpose of collecting the information. Seeking consent may be impossible or inappropriate when the individual is a minor, seriously ill, or mentally incapacitated. In addition, organizations that do not have a direct relationship with the individual may not always be able to seek consent. For example, seeking consent may be impractical for a charity or a direct-marketing firm that wishes to acquire a mailing list from another organization. In such cases, the organization providing the list would be expected to obtain consent before disclosing personal information.

³⁴ This doctrine is sometimes referred to as "common law illegality." See Fridman, *supra* note 16 at 390-436.

³⁵ *Ibid.* at 391.

³⁶ *Egerton v. Brownlow* (1853), 4 H.L. Cas. 1, 10 E.R. 359 at 437 (H.L.): "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."

³⁷ *Supra* note 2.

Recommendation #7

Amend PIPEDA to include a provision stipulating that:

Contracts containing a waiver of privacy or otherwise requiring an individual to contract out of privacy protections provided for in this Act shall not be enforceable where the contract: (i) fails to meet PIPEDA's threshold for consent, (ii) is otherwise in contravention of Canadian privacy law, or (iii) where there are other pressing public policy considerations.³⁸

An express provision along these lines is 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. A provision of this sort is further justified by 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, Principle 4.3.3.

A more specific and fundamental revision is also necessary to ensure that organizations are not permitted to use standard form contracts to undermine an individual's ability to withdraw consent to the collection, use or disclosure of personal information. PIPEDA's Principle 4.3.8 creates a right to withdraw consent, but is silent on whether it is possible to contract out of that right. It is recommended that the language in this provision be amended to clarify that one cannot contract out of the right to withdraw consent. The British Columbia legislation provides a clear model.

Recommendation #8

Amend PIPEDA Principle 4.3.8 to include a paragraph stipulating that:

[a]n organization must not prohibit an individual from withdrawing his or her consent to the collection, use or disclosure of personal information related to the individual.³⁹

Finally, it is important to note that many of the above recommendations will only be effective if appropriate penalties or remedies for the circumvention of privacy laws are also provided. The Privacy Commissioner cannot currently order damage awards,⁴⁰ nor does the Privacy Commissioner seem to want such additional powers.⁴¹

³⁸ See *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.

³⁹ BC PIPA, *supra* note 10 at s. 9(3).

⁴⁰ See Privacy Commissioner of Canada, *Annual Report to Parliament 2003-2004* (November 2004) online: <http://www.privcom.gc.ca/information/ar/200304/200304_e.asp> at 58;

Recommendation #9

Amend PIPEDA so that it provides the Privacy Commissioner (or an associated Tribunal) with order-making powers, including the power to award damages.

In this context it is useful to note that, of the more than fourteen hundred complaints that the Privacy Commissioner has received, only nine cases have been commented on by the Federal Court.⁴² Not a single one of these six cases has attracted a damage award. Three of the complainants were able to recoup their costs.⁴³ Four cases saw the court awarding no costs to either party. In two cases, the complainant had to bear his as well as his opponent's legal costs.⁴⁴

Privacy Commissioner of Canada, *Annual Report to Parliament 2002-2003* (September 2003) online: <http://www.privcom.gc.ca/information/ar/02_04_11_e.asp> at 57; Privacy Commissioner of Canada, *Annual Report to Parliament 2001-2002* (January 2003) online: <http://www.privcom.gc.ca/information/ar/02_04_10_e.asp> at 59.

⁴¹ Privacy Commissioner of Canada, *Statutory Review of the Personal Information Protection and Electronic Documents*, online:

<http://www.privcom.gc.ca/parl/2006/parl_061127_e.asp>.

⁴² *Blood Tribe Department of Health v. Privacy Commissioner of Canada* 2005 FCT 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 FCT 852 [Erwin Eastmond]; *Janice Morgan v. Alta Flights (Charters) Inc.* 2005 FCT 421; *Mathew Englander v. Telus Communications Inc. and Privacy Commissioner of Canada* 2004 FCA 387 [Englander]; *Ronald G. Maheu v. IMS Health Canada and the Privacy Commissioner of Canada* 2003 FCT 1 [Maheu]; *Rousseau v. Wyndowe* 2006; *Funk v. Bank of Montreal* 2006 FC 1266 [Funk]; *Vanderbeke v. Royal Bank of Canada* 2006 [Vanderbeke].

⁴³ *Englander, Maheu and Funk*, *supra* note 46.

⁴⁴ *Erwin Eastmond and Vanderbeke*, *supra* note 46.