



Canadian Internet Policy and Public Interest Clinic
Clinique d'intérêt public et de politique d'internet du Canada

**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")***

November 28, 2006

Canadian Internet Policy and Public Interest Clinic (CIPPIC)
University of Ottawa, Faculty of Law
57 Louis Pasteur, Ottawa, ON K1N 6N5
tel: 613-562-5800 x2553
fax: 613-562-5417
www.cippic.ca

Executive Summary

It has now been almost six years since the *Personal Information Protection and Electronic Documents Act* ("PIPEDA") came into force for federally-regulated organizations. The PIPEDA review presents an important opportunity for the government to improve upon a statute that was experimental in many respects, and whose shortcomings have become obvious to many over the first few years of its operation.

Earlier this year, CIPPIC conducted a major study of retailer compliance with PIPEDA. The study indicated high levels of non-compliance with the Act. Our experience and research suggest that, while the Act has had an important and positive impact on marketplace privacy in Canada, both the ombuds model approach and the vagueness (or in some cases absence) of key substantive obligations in the Act have seriously compromised the Act's effectiveness.

We therefore propose a number of amendments designed to clarify rights and obligations, to close gaps, and to give the regime the "teeth" it is clearly lacking. Such amendments include:

- giving the Commissioner (or an associated Tribunal) order-making powers;
- reducing barriers to the enforcement of PIPEDA rights via Federal Court;
- permitting class actions under PIPEDA;
- providing for punitive as well as compensatory damages in court;
- mandatory naming of respondents in published Commissioner findings;
- mandatory Commissioner reporting on complaints;
- expanding the list of offences under PIPEDA;
- removing the "reasonable grounds" requirement for audits; and
- giving the Commissioner powers to share information with her counterparts.

While PIPEDA's redress and enforcement regime is most need of reform, some important substantive provisions of the Act suffer from lack of clarity, and others leave strange gaps. We have therefore proposed amendments to clarify and add provisions dealing with:

- the criteria for valid consent;
- data breach notification;
- reasonable limits on collection, use and disclosure;
- children's privacy;
- openness and individual access;
- attempted collection, use and disclosure;
- state surveillance; and
- the definition of "organization".

CIPPIC

The Canadian Internet Policy and Public Interest Clinic (CIPPIC), based at the University of Ottawa, Faculty of Law, seeks to ensure balance in policy and law-making processes by representing under-represented interests on issues that arise as a result of new technologies. Upper year law students work under the supervision of the Clinic director and staff counsel on projects and cases involving the intersection of law, technology and the public interest. CIPPIC engages in policy development, legislative advocacy, public education, client advice, and precedent-setting litigation. Issues addressed include privacy, copyright, free speech, domain name governance, and consumer e-commerce. Many clients come to the clinic for advice on privacy-related matters.

In addition to its ground-breaking reports on retailer compliance with PIPEDA and on the Canadian data brokerage industry, CIPPIC has lodged six policy-related complaints under PIPEDA with the Office of the Privacy Commissioner, and has applied to the Federal Court for judicial review of the Privacy Commissioner's refusal to accept jurisdiction in one of these cases. CIPPIC has also submitted comments to policy-makers on PIPEDA's regulation re: "investigative bodies" and on the "substantial similarity" of Ontario's health privacy legislation with PIPEDA. For more information, see www.cippic.ca (under "Projects – Privacy").

Philippa Lawson, Executive Director and General Counsel, CIPPIC

Philippa Lawson is a nationally recognized privacy lawyer and advocate. She has worked with Canadian and international consumer organizations since the early 1990s on many privacy-related issues, including the regulation of Caller ID and telemarketing, the development of the CSA Privacy Code, and implementation of federal private sector data protection legislation ("PIPEDA"). Prior to starting up CIPPIC in 2003, she was senior counsel for the Public Interest Advocacy Centre. She is a member of the CSA Committee on the Model Privacy Code, is a co-investigator/collaborator on the SSHRC-funded "[On The Identity Trail](#)" project, and is the lead investigator for the research project "Legal and Policy Approaches to Identity Theft" funded by the Ontario Research Network on Electronic Commerce (ORNEC). Her most recent publications include *On the Data Trail*, an exposé of the Canadian data brokerage industry, and *Compliance with Canadian Data Protection Laws: Are Retailers Measuring Up?*, a report on the first major assessment of industry compliance with privacy laws in Canada. Both reports, published in May 2006, are available on the CIPPIC website. Ms. Lawson continues to be actively engaged in privacy-related research and advocacy from the public interest perspective, and is frequently quoted in the media on privacy-related issues.

Table of Contents

Introduction.....	1
Redress and Enforcement Regime	1
<i>PIPEDA's enforcement regime is ineffective</i>	<i>1</i>
<i>A strict "ombuds" model is inappropriate for regulation of the private sector</i>	<i>2</i>
<i>Strong enforcement powers are compatible with conciliatory approaches to compliance</i>	<i>3</i>
<i>Options for improved incentives and enforcement</i>	<i>3</i>
ORDER-MAKING POWERS	4
STATUTORY RIGHTS OF ACTION TO FEDERAL COURT	4
NAMING OF RESPONDENTS IN PUBLISHED DECISIONS.....	6
COMMISSIONER REPORTING ON COMPLAINTS.....	7
OFFENCES AND PENALTIES	7
COMMISSIONER POWERS TO SHARE INFORMATION.....	8
AUDITS	8
Substantive Provisions	9
DATA BREACH NOTIFICATION	9
CONSENT	10
REASONABLE LIMITS	13
CHILDREN'S PRIVACY	15
OPENNESS AND INDIVIDUAL ACCESS	16
ATTEMPTED COLLECTION, USE OR DISCLOSURE	16
STATE SURVEILLANCE	17
DEFINITION OF "ORGANIZATION"	18
Recommendations.....	19

Introduction

It has now been almost six years since the *Personal Information Protection and Electronic Documents Act* ("PIPEDA") came into force for federally-regulated organizations. The PIPEDA review presents an important opportunity for the government to improve upon a statute that was experimental in many respects, and whose shortcomings have become obvious to many over the first few years of its operation.

The Act was unusual insofar as it adopted a "light-handed" ombuds model for private sector regulation, along with an industry-wide voluntary code of practice as its set of key substantive obligations. Both approaches were questioned at the time the proposed legislation was under consideration. It is an appropriate time now to review how effective these approaches have been, and what specific problems have been encountered in their implementation.

Our experience with PIPEDA and our research into retailer compliance with the Act suggest that, while the Act has had an important and positive impact on marketplace privacy in Canada, both the ombuds model approach and the vagueness (or in some cases absence) of key substantive obligations in the Act have seriously compromised the Act's effectiveness. We therefore propose a number of amendments designed to clarify rights and obligations, to close gaps, and to give the regime the "teeth" it is clearly lacking.

Redress and Enforcement Regime

This, in our view, is the single most important issue for consideration in the PIPEDA review. While many substantive provisions of the Act can and should be improved (see below), the Act's approach to redress and enforcement is badly in need of reform. There is no point in having a law that is widely disrespected because it lacks incentives to comply.

PIPEDA's enforcement regime is ineffective

Anecdotal evidence suggesting widespread non-compliance with the Act was confirmed earlier this year by the results of a rigorous study conducted by CIPPIC over the fall of 2005 and winter of 2006.¹ The study, the first ever significant survey of business compliance with the Act, focused on retailer compliance with four basic requirements of PIPEDA: openness, accountability, individual access, and consent. A total of 64 retailers were assessed (72 in the case of individual access). In short, the results indicated widespread non-compliance in all four areas, by large as well as small organizations.

Others have noted that under the current regime, "regulated parties are able to ignore the Commissioner's decisions with impunity",² "[business] implementation of the PIPED Act

¹ *Compliance with Canadian Data Protection Laws: Are Retailers Measuring Up?* (CIPPIC, May 2006).

² BCCLA, *Securing Compliance, Protecting Privacy: The PIPEDA Enforcement Evaluation Project* (March 2006), p.83.

has been *ad hoc* at best and non-existent at worst",³ companies found in violation of the Act remain non-compliant,⁴ and "for many organizations privacy compliance has ceased to be a serious legal obligation. Instead, for many it is considered a business risk that carries no realistic expectation of serious financial consequences or diminished reputation — a risk that can be managed through minimal compliance and contrition if caught".⁵ There can be little dispute that the current model is insufficiently effective and that change is needed.

A strict "ombuds" model is inappropriate for regulation of the private sector

The current compliance/enforcement regime under PIPEDA has been characterized as an ombuds model, under which complaints are made to the Commissioner, who has broad powers to investigate, to resolve complaints via mediation or conciliation, to initiate her own complaints, and to engage in audits, but whose findings are not binding. The Commissioner is vested with powers to publicize "information relating to the personal information management practices of an organization if [she] considers that it is in the public interest to do so", but is otherwise required to keep all information obtained in the course of her investigations confidential. In addition to these largely discretionary powers (other than mandatory investigation of complaints), the Commissioner is required to engage in research, public education, and promotion of data protection practices.

In order to obtain a legally binding ruling or order, complainants (or the Commissioner) must apply to Federal Court, after the Commissioner has reported on the complaint. The Court then treats the case *de novo*, and may award damages in addition to other remedies.

The pure ombuds model was developed and is typically employed in two contexts: by governments to regulate public administration, and by private sector organizations to regulate themselves. It makes sense in those contexts: where the regulated entity has a public interest mandate (in the case of government), or where the regulated entity is subject to other, overriding laws and regulations (in the case of private organizations). Neither of these conditions apply here: PIPEDA is *government* regulation of *private sector* activity.

Indeed, some sectors (such as banking) have their own, pre-existing ombudsmen who already fulfil the ombuds role. What is needed for effective data protection is not so much an additional ombudsperson to resolve individual complaints, but rather a regulator with the mandate, the powers and the will to enforce, as well as to encourage, widespread compliance with the Act.

The pure ombuds approach focusing on individual complaint resolution in confidence is particularly unsuitable in the case of business practices affecting large numbers of

³ "Implementing PIPEDA: A review of internet privacy statements and on-line practices", University of Toronto Centre for Innovation Law and Policy (May 6, 2005), quote from Executive Summary; <<http://pipedaproject.rcat.utoronto.ca/>>

⁴ John Lawford, *Consumer Privacy under PIPEDA: How are we doing?* (PIAC: Nov.2004), pp.44-55.

⁵ "Rising to the Privacy Reform Challenge", *Toronto Star* (Oct.25, 2004).

consumers, where the primary goal of the legislation is to change industry behaviour. Dispute resolution should be a lower priority, although individuals should have access to some low cost, efficient and effective means of obtaining redress for privacy violations. It is also unsuitable in contexts such as the present where industry needs clear and useful guidance in the form of detailed findings, advance rulings, and interpretation bulletins.

Strong enforcement powers are compatible with conciliatory approaches to compliance

It has been suggested that a pure ombuds model focusing on individual complaint resolution, conciliation, and persuasion cannot be combined with a more traditional regulatory model under which the regulator makes binding orders, publishes decisions, and imposes penalties for non-compliance. While combining these two functions may pose some challenges, is it clearly not impossible. Other data protection regulators, including all three provincial commissioners, do so in various ways, with good results.

Indeed, the experience in Alberta suggests that "the combination of a mediation-first philosophy and fairly significant enforcement powers (particularly the willingness to name and the ability to issue binding orders) creates a climate that fosters business compliance; most organizations that are contacted by the Alberta Office want to comply with the law and to be given the tools and guidance to do so."⁶ Other regulators such as the CRTC, Competition Bureau, and Canadian Human Rights Commission, all engage in ombuds-type functions at the same time as they wield strong enforcement powers, either directly or via a specialized tribunal.

Clearly, there is no "either/or" choice to be made between a privacy ombudsman and a privacy enforcer: experience proves that both approaches can coexist within the same agency. Moreover, experience strongly suggests that the effectiveness of private sector privacy regulation will be enhanced by a regime that combines elements of both models.

Options for improved incentives and enforcement

A variety of tools and mechanisms for improving compliance with PIPEDA are possible. They include:

- Commissioner use of the subs.20(2) power of publicity to "name and shame" organizations who fail to comply with the Act;
- greater Commissioner use of audit powers both for random "spot checks" and for more in-depth audits of organizations against whom complaints have been made;
- providing the Commissioner with order-making powers (as is the case in all three provinces with similar data protection laws);
- establishing a new Tribunal with order-making powers, to which complainants and/or the Commissioner can take unresolved complaints and obtain damages;
- providing individuals and classes of individuals with a statutory right of action through which they can hold organizations accountable and obtain damages;

⁶ BCCLA, *op cit*, p.41.

- allowing organizations (e.g., CIPPIC) and groups of individuals to lodge complaints and obtain injunctive relief on behalf of others;
- allowing for punitive as well as compensatory damages;
- treating willful contraventions of the Act and/or failure to comply with Commissioner orders as offences, subject to financial penalties.

These options are not all mutually exclusive. A combination of enforcement and redress mechanisms will be most effective. Moreover, there is no single "right" approach to redress and enforcement of data protection laws; existing models in other jurisdictions provide useful points of comparison and have their own strengths and weaknesses.

Order-Making Powers

Our review of approaches in other jurisdictions and sectors suggests that the Alberta and B.C. models of private sector data protection⁷ warrant close consideration. These two statutes were drafted three years after PIPEDA with a view to improving upon PIPEDA while passing the "substantial similarity" test. In our view they have indeed improved upon PIPEDA in numerous respects, including the enforcement model. One concern that we do however have with these models is the right of the Commissioner to ignore complaints and the lack of any alternative redress mechanism for complainants who cannot convince the Commissioner to take on their cases.

Recommendation #1:

Give the Privacy Commissioner (or an associated Tribunal) order-making powers, similar to those of the Alberta and B.C. Commissioners.

Recommendation #2:

Should PIPEDA be amended to give the Commissioner discretion with respect to the investigation of complaints, it should be further amended to require that the Commissioner respond in writing to each complainant within 30 days of the complaint, setting out whether or not the complaint will be investigated. This would free complainants up to pursue the matter in court if the Commissioner chooses not to inquire into their complaints.

Statutory Rights of Action to Federal Court

The current enforcement mechanism relies on individual complainants taking cases to Federal Court. Individuals who want compensation for losses due to a breach of PIPEDA or who simply want to hold organizations accountable under the Act must apply to

⁷ Alberta *Personal Information Protection Act*, S.A. 2003, c.P-6.5; British Columbia *Personal Information Protection Act*, S.B.C. 2003, c.63.

Federal Court, after waiting up to a year (and sometimes longer) for a finding from the Privacy Commissioner. Yet, applications to Federal Court are beyond the means of most individuals. The cost of a privacy lawsuit will usually far outweigh likely recoverable damages. Moreover, should the applicant lose in court, he or she may be liable for the other party's costs. This was the case for Mathew Englander, who eventually won his case upon appeal, but not until after being assessed several thousand dollars of costs by the trial level court.

Adding to this cost/risk barrier is the fact that court records are a matter of public record. Many legitimate complaints under PIPEDA involve very private information that the complainant may not wish to and should not have to expose to public scrutiny.

Individuals should have access to a low risk, low cost avenue (e.g, Tribunal or simplified Federal Court procedure) by which to hold organizations accountable and to obtain damages for breaches of the Act, without having to make their names public.

Recommendation #3:

If PIPEDA is amended to give the Commissioner order-making powers, include a statutory right of action for damages for successful complainant via an expedited procedure in Federal Court (or Tribunal), under which applicants are insulated from adverse costs orders and are entitled to solicitor-client costs should they succeed in obtaining damages.

If the current redress/enforcement regime is retained, amend s.14 of PIPEDA to protect *bona fide* applicants from adverse cost awards in Federal Court, and provide for solicitor-client costs in the event of successful applications.

Whether or not the redress/enforcement regime is changed, protect individual applicants for judicial review of Commissioner decisions from adverse cost awards other than in exceptional circumstances.

Recommendation #4:

Protect complainant privacy by requiring the Federal Court (or Tribunal) not to publish any identifying information about complainants in applications for damages, enforcement, judicial review, or otherwise.

Punitive damages are appropriate in cases “where the combined award of general damages and aggravated damages would be insufficient to achieve the goal of punishment and deterrence”.⁸ In the context of privacy breaches, quantifiable damages are often minimal or non-existent even though the violation may be egregious. Punitive damages may be the only meaningful remedy for complainants under PIPEDA. Without the possibility of punitive damages, even the most meritorious and compelling cases may

⁸ *Hill v. Church of Scientology of Toronto and Manning*, [1995] 2 S.C.R. 1130 at 1208-1209, (per Cory J.)

not be brought, simply because of the difficulty proving damages or the potentially low dollar awards for privacy breaches.

Recommendation #5:

Provide for punitive as well as compensatory damages under s.16 of PIPEDA.

PIPEDA's focus on individual complaints and individual court actions does not reflect the often widespread nature and impact of privacy-related invasions. It fails to provide an effective redress mechanism for individuals in such cases – especially where the cost of proceeding in court drastically outweighs the potential recovery by the individual complainant. Nor does it take advantage of the strong compliance incentive posed by potential class actions, especially where individual damages are minimal - as is so often the case with privacy invasions. Class actions discipline non-compliant companies in cases where individual actions would not proceed or where even successful individual actions would make no difference to the company's practice.

Section 11 requires that complainants be "individuals", and s.14 permits only complainants (having received a Commissioner report on their complaint) to apply to court for a binding determination and/or damages. This restriction effectively denies recourse to other similarly affected individuals who may wish to take the case to Court on their own behalf or on behalf of others, and who should have the right to do so without having first to lodge a duplicating complaint with the Privacy Commissioner.

Recommendation #6:

Permit class actions under s.14 of the current model or under a new statutory right of action, if adopted. Further amend s.14 to permit Federal Court applications by similarly affected individuals, not just those complainants who lodged the complaint in question.

Naming of Respondents in Published Decisions

Providing the Commissioner with the power to order injunctive relief is first step toward giving PIPEDA the teeth it needs. However, merely being ordered to comply is not a sufficient deterrent; organizations need to know that they risk reputational and/or financial damage if they fail to comply with the law. The Commissioner should publish full decisions on complaints that have not been resolved via mediation as a matter of course. Such decisions should include the names of organizations but should protect the privacy of complainants by not including any identifying information about them.

While s.20 of PIPEDA allows such publication, all federal Privacy Commissioners to date have taken the position that the routine publication of organization names in

PIPEDA findings is not in the public interest. We respectfully disagree, and note that Commissioners in Alberta and B.C. publish this information as a matter of course.

Publication of full decisions with names of organizations also serves to provide the guidance that industry needs in order to understand their obligations under the Act.

Recommendation #7:

Amend s. 20 of PIPEDA to require publication by the Commissioner of full decisions, including names of organizations, but not including identifying information about complainants.

Commissioner Reporting on Complaints

It is important that Parliament and the public be able to assess the performance of the Office of the Privacy Commissioner in terms of complaints handled and resolution thereof. This is particularly important if the Commissioner is given discretion not to investigate complaints.

Recommendation #8

Amend s.25 of PIPEDA to require specific annual reporting by the Commissioner on the type, treatment, and resolution of all complaints received. Such reporting should include the total number of complaints received, the number of complaints not investigated, the number of complaints for which resolution was attempted via mediation or conciliation, and the number that were ultimately decided by way of orders or findings.

Offences and Penalties

PIPEDA creates offences for obstructing the Commissioner in investigations or audits, willfully destroying information that is the subject of an access request, and discriminating against whistleblowers (s.28). In contrast, Alberta and B.C. treat the following additional actions or omissions as offences:

- using deception or coercion to collect personal information in contravention of the Act (B.C.)
- willfully collecting, using or disclosing personal information in contravention of the Act (Alberta)
- knowingly misleading the Commissioner in the course of his or her duties under the Act;
- failing to comply with an order made by the Commisisoner under the Act.

In all cases, the offences are punishable by penalties of up to \$10,000 for individuals and \$100,000 for organizations

Although these criminal law powers may be rarely employed, they do send a signal to organizations that their obligations under the Act are not trivial. They also permit state action to enforce the Act in appropriate cases.

Recommendation #9:

Expand s.28 of PIPEDA to cover willful violations of the Act, knowingly misleading the Commissioner, and (if the Commissioner or a Tribunal is granted order-making powers), failing to comply with such orders.

Commissioner Powers to Share Information

Increasingly, data is flowing across borders for commercial purposes, and organizations based outside Canada are reaching into Canada in order to collect and disclose personal information about Canadians. While the Commissioner may have jurisdiction over foreign entities in such situations (given a "real and substantial connection" to Canada), enforcing a Canadian court or Commissioner order against an entity wholly based outside Canada could prove difficult. The Commissioner should therefore be permitted to share information and cooperate in joint investigations with counterparts in other jurisdictions, including those without "substantially similar" data protection legislation. Such a power would enhance the Commissioner's ability to oversee and enforce the law, and is unlikely to be abused.

Recommendation #10:

Amend PIPEDA to explicitly permit the Commissioner to share information and cooperate in investigations with counterparts in other countries and in all provinces in Canada.

Audits

PIPEDA provides the Commissioner with the power to audit organizations where she "has reasonable grounds to believe that the organization has been contravening [the Act]".⁹ Audits, both full-scale and in the form of relatively quick site visits, can be very effective ways of educating industry as well as encouraging compliance. Yet this compliance tool has remained largely unused, apparently because of concerns about the "reasonable grounds" threshold for exercising it.

Such concerns proved warranted when just a few weeks ago, Equifax sued the Commissioner in an effort to shut down an intended audit on the basis that the

⁹ subs.18(1)

Commissioner lacked "reasonable grounds". Equifax sued despite the fact that that OPC had received four separate complaints about Equifax and had conducted its own initial investigation before launching the audit.

It is not clear why "reasonable grounds" should be required for an audit; there are good reasons for allowing the OPC to engage in audits of any organizations at any time. The agency is accountable to Parliament for its actions and is unlikely to abuse this power.

Recommendation #11:

Remove the "reasonable grounds" requirement for audits.

Substantive Provisions

Data Breach Notification

Identity theft and related fraud has become a serious risk for individuals in the information age. Phonebusters, a Canadian law enforcement and public education initiative, reported over 11,000 complaints from ID theft victims in 2005. In the U.S., ID theft-related frauds have topped the FTC's list of consumer complaints for years.

While some ID thieves gather data directly from individuals' wallets, magnetic stripe cards, mail, and garbage, many seek opportunities to steal such information from organizations that hold large quantities of valuable personal information in computer databases. They have succeeded in gathering data by such means as bribing insiders, posing as legitimate business customers in order to get access to the database, hacking into computer databases (or taking advantage of security holes), and combing through discarded records and computer equipment.

Clearly, there is no incentive for the organization that has suffered such a security breach to disclose this fact publicly: it can lead to serious reputational harm. This problem was illustrated nicely just a couple of years ago when Choicepoint, a giant databroker in the USA, discovered that it had unwittingly granted access to its database to criminals. Rather than notifying all affected individuals, however, Choicepoint initially notified only those individuals resident in California, which was at the time the only state in the USA to require such notification. Only after enormous public outcry did Choicepoint notify the remaining affected individuals. Since that event, most states in the USA have adopted breach notification laws similar to that of California.¹⁰

California's law¹¹ requires notification to California residents of any security breach that results in the acquisition of unencrypted personal information by an unauthorized person,

¹⁰ See CIPPIC's Working Paper on "Approaches to Data Breach Notification", forthcoming.

¹¹ California Civil Code, ss.1798.29, 1798.82-1798.84.

as long as the compromised information includes an individual's first name or initial and last name, in combination with any of the following:

- 1) Social security number,
- 2) Driver's license number or California Identification Card number, or
- 3) Account number, credit or debit card number, in combination with any required security code, access code, or password that would permit access to an individual's financial account.

The California law also sets out procedures and timelines for notification.

If organizations are under a legal requirement to report security breaches, they will be more inclined to take the necessary steps to ensure proper security throughout their operations. PIPEDA includes a general requirement to "protect personal information against loss or theft..." (4.7.1) but does not include any specific data breach notification requirement. The only statute to include such a rule currently is Ontario's *Personal Health Information Protection Act*.¹² We advocate adopting a data breach notification rule, modeled on the California law, in PIPEDA.

Recommendation #12:

Amend Principle 7 of PIPEDA to include a requirement to notify affected individuals of a security breach that results in the acquisition of unencrypted personal information by an unauthorized person. Such requirement should include specifics regarding the type of personal information and breach that triggers the obligation to notify, form and content of notices, timing of notices, who should be notified, etc.

Failure to notify affected individuals as required under the Act should be subject to tough penalties.

Consent

PIPEDA is a consent-based model of data protection: subject to some limits, it permits collection, use and disclosure of personal information for commercial purposes as long as the individual has consented. But the CIPPIC study of retailer compliance with PIPEDA shows that a large proportion (possibly a majority) of organizations are not obtaining meaningful consent to secondary uses and disclosures of consumer information. Most companies rely on "opt-out" consent, but fail to bring the opt-out and related information to the customer's attention. Many use "blanket consent" clauses giving themselves broad, unspecified rights to use and disclose the information as they wish. Such clauses clearly subvert the intent of PIPEDA and render the concept of consent meaningless.

Almost one-third of the companies we assessed failed to notify consumers of their data practices during the ordering process. Of those that did notify and offer an opt-out during

¹² S.O. 2004, c.3, Sch.A.

the ordering process, 50% did so merely via a link to the privacy policy, and a majority of these failed to bring the link to the customer's attention.

Privacy policies themselves are often unclear or incomplete, such that individuals cannot determine how their information will be used or to whom it will be disclosed. Although most companies we assessed included an opt-out in their privacy policy, 60% buried it inconspicuously in the policy. A number of companies required consent to unnecessary uses or disclosures in order for the consumer to transact, violating PIPEDA's "refusal to deal" section. A disturbing number of policies we reviewed are misleading, suggesting that consumer information will not be used for secondary purposes when in fact it will.

In addition to the incentive/enforcement problem described above, our findings suggest that some organizations lack an understanding of the need for *informed* consent, the differences between opt-in and opt-out consent, and the criteria for valid opt-out consent (which the Commissioner has set out in public findings).

This could be due to PIPEDA's vague and round-about provisions regarding consent. Nowhere does the Act define "consent" or set out clear preconditions and criteria for each of the three forms of consent (express, implied, deemed/opt-out). Leaving such key guidelines to Commissioner and court jurisprudence is unnecessary and puts organizations to greater expense in their efforts to comply with the Act.

The concept of notice, so critical to informed consent, is almost missing from PIPEDA: organizations are merely required to "make a reasonable effort to ensure that the individual is advised..." (4.3.2). In our study of retailer compliance, we found a number of instances in which companies provide consumers with an opt-out during the ordering process, but no clear notice of the uses/disclosures in which the company engages.

Both Alberta and B.C. have substantially improved upon PIPEDA's drafting of consent-related provisions. In particular, both provincial Acts set out clear requirements for valid consent, which requirements include notice on or before collection. Both also clearly distinguish between express, implied, and deemed/opt-out consent, setting out different sets of requirements for each. We strongly recommend the Alberta and B.C. approach to consent requirements. Whether or not such an approach is adopted, certain consent-related provisions of PIPEDA need to be drafted to provide clearer guidance to the private sector and to close gaps in the current regime.

Recommendation #13:

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 "Organizations 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 #14

Amend the poorly drafted "refusal to deal" section in PIPEDA (Principle 4.3.3) to replace "...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 #15

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 PIPAs¹³).

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".

Much of the trade in personal information involves organizations collecting the data from other organizations, who may have collected it from still other organizations, etc., such that the ultimate uses and disclosures of one's personal information are very remote from the original collection at which time consent was supposedly obtained. Principle 3 of the CSA Code contains a "Note" addressing this situation among others, and stating that "in such cases, the organization providing [a mailing list for direct marketing] would be expected to obtain consent before disclosing personal information." This note was not incorporated into PIPEDA, such that the issue of indirect collection and consumer consent remains unaddressed in the legislation.

Recommendation #16

Include in Principle 4.4 of PIPEDA a requirement that personal information be collected directly from the individual unless the individual has consented to the 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)).

In many cases we have encountered, organizations obtaining consent via an opt-out process require that individuals initially consent to secondary uses and disclosures against

¹³ Alberta *Personal Information Protection Act*, S.A. 2003, c.P-6.5; British Columbia *Personal Information Protection Act*, S.B.C. 2003, c.63.

their will (wittingly or unwittingly), and opt-out later through a process entirely separate from the transaction. This common trick of separating the opt-out from the initial consent places an undue burden on individuals to withdraw consent that they never actually provided in the first place, and increases the likelihood that consent is being incorrectly assumed. Those individuals who do go to the trouble of opting-out are forced to accept a temporary period during which their consent is wrongly assumed. This is unfair to individuals and unnecessary on the part of organizations. Individuals should be presented with the opt-out option at the time and in the medium that an organization notifies the individual that their consent is being assumed. The opt-out should immediately follow the notice and should be easily executable in that medium.

Recommendation #17:

In Principle 4.3.1, replace the two last sentences “Typically, 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.”

It appears that there was an oversight in the drafting of PIPEDA's Regulations specifying "publicly available" information (SOR/2001-7), leading to the strange and undesirable result that individuals do not have a right under PIPEDA to opt-out of secondary uses of their information published in telephone directories. While telephone companies may be offering subscribers such an opt-out, this should be more than a voluntary measure.

Recommendation #18:

Amend s.1(a) of PIPEDA's Regulations specifying "publicly available" information (SOR/2001-7) to allow individuals to opt-out of secondary uses of their information published in the telephone directory.

Reasonable Limits

The CSA Code on which PIPEDA is based lacks a very significant protection: limits on the purposes for which organizations can collect, use and disclose personal information. Especially where consent is obtained through opt-out processes such that the individual may be consenting unwittingly, it is essential that there are fundamental limits on the purposes for which organizations collect personal information and the practices that they can legally engage in.

Subsection 5(3) was added to PIPEDA for this reason. It limits organizations' right to collect, use and disclose personal information to "only [those] purposes that a reasonable person would consider are appropriate in the circumstances". This provision has proven

to be critical in the resolution of numerous complaints under PIPEDA, and has allowed the Commissioner to engage in a "balancing test" in order to determine whether the purpose in question meets the reasonableness/appropriateness test, apart from any issue of consent.

Subs.5(3) is, however, strangely limited to *purposes* even though many appropriateness concerns (e.g., inappropriate disclosure by debt collectors) revolve around *practices*. It is also very vague, causing uncertainty for organizations. The addition of a statutory test and some non-exclusive examples of inappropriate use and disclosure would be helpful in this regard. Such examples should include:

- (a) collection, use, or disclosure of personal information about persons under the age of 16, except where explicitly authorized by parents or guardians;
- (b) collection, use or disclosure of personal information when non-personal information would have sufficed;
- (c) disclosure of personal information by debt collectors to third parties;
- (d) disclosure of personal credit information by credit bureaus other than for the purpose of assessing an individual's credit rating.

Recommendation #19:

Amend subsection 5(3) to cover practices as well as purposes. Suggested drafting:
"An organization may collect, use or disclose personal information only for purposes *and only in a manner and to an extent that a reasonable person would consider are appropriate in the circumstances.*"

Alternatively, adopt the Alberta approach, under which both purposes and practices are subject to a "reasonableness" test (see ss.11(2), 16(2), 19(2), Alta PIPA).

Specify components of the "reasonableness" test as follows:

- (a) rational connection of the collection, use or disclosure to a reasonable purpose;**
- (b) minimal impairment of the individual's privacy rights in achieving that purpose; and**
- (c) proportionality as between the commercial purpose and the loss of individual privacy.**

Include a new clause in subsection 5(3), setting out examples of inappropriate collection, use and disclosure. Suggested drafting: "For greater certainty, the following purposes and practices would not be considered appropriate by reasonable persons...."

Children's Privacy

PIPEDA is silent as to the treatment of the personal information of minors. Instead, it applies the same consent-based rules and "bottom line" protections to adults and children alike. Whether or not a given practice involving the collection, use or disclosure of children's data would be considered appropriate in the circumstances under subs.5(3) is left to conjecture. As a result, there is considerable uncertainty in the marketplace, with unfortunate implications for children's privacy rights. Websites aimed at young children and teens are proliferating. We have received complaints about commercial websites that engage in financial and other transactions with children without parental approval.

The Canadian marketplace appears tremendously confused about the mechanics of obtaining a legally binding consent to the collection, use and disclosure of the personal information of a minor. Can a minor provide such consent? If not, must the marketer obtain the consent of the minor's legal guardian? Does the minor's age make a difference – should we treat seventeen year-olds the same as seven year-olds?

The United States has seen fit to legislate specifically on the issue of children's privacy: the *Children's Online Privacy Protection Act*, effective April 21, 2000, applies to the online collection of personal information from children under 13. It spells out what a Web site operator must include in a privacy policy, when and how to seek verifiable consent from a parent, and what responsibilities an operator has to protect children's privacy and safety online. Canada has no such legislation.

The Canadian Marketing Association's Code of Ethics includes guidelines for marketing to children¹⁴, applying different rules depending on the age of the child. The Canadian Code of Practice for Consumer Protection in Electronic Commerce¹⁵ sets out limits on the collection of children's personal information online, but does not address age thresholds. These self-regulatory efforts go some way towards limiting the inappropriate collection, use and disclosure of children's information, but clearly do not affect those organizations who are not members of CMA or do not subscribe to the Code of Practice, and may have accepted standards of practice that are unacceptable to most Canadians.

Recommendation #20:

Include in PIPEDA specific rules limiting the collection, use and disclosure of children's personal information. Such rules should be at least as strict as those already adopted in the *Canadian Code of Practice for Consumer Protection in Electronic Commerce* and by the Canadian Marketing Association. There should be strict and significant penalties for violating these provisions.

¹⁴ <http://www.the-cma.org/regulatory/codeofethics.cfm>

¹⁵ <http://cmcweb.ca/epic/internet/incmc-cmc.nsf/en/fe00073e.html>

Openness and Individual Access

Our study highlighted two strange gaps in the openness and individual access principles under PIPEDA. Principle 4.8.2(e) requires that organizations state what personal information is made available to "related organizations (e.g., subsidiaries)". This provision is important insofar as organizations treat corporate affiliates as part of the same organization for the purposes of PIPEDA. However, it strangely ignores disclosures to unaffiliated third parties. Based on the results of our study, most organizations share customer information with unrelated third parties. Organizations should be required to give consumers clear notice of all personal information disclosures they make to third parties, related and unrelated.

The list of required disclosures in Principle 4.8.2, as well as in response to access requests under Principle 4.9.1, does not include sources. Individuals should have the right to know from what sources an organization has obtained information about them.

Recommendation #21:

Amend Principle 4.8.2(e) to replace "related organizations" with "third parties, including related organizations".

Amend Principle 4.8 to include a new clause requiring disclosure of "sources other than the individual from which the organization obtains personal information."

Amend Principle 4.9.1 to replace "Organizations are encouraged to indicate the source of this information" with "Upon request and to the extent possible, organizations shall disclose all sources from which they have obtained personal information about the individual."

Attempted Collection, Use or Disclosure

One of the few cases under PIPEDA that has been decided by the Federal Court involved a clear case of attempted collection of personal information (via a tape recorder) without the individual's knowledge or consent. The Federal Court of Appeal¹⁶ found that even if the collection would have breached PIPEDA had it taken place, *PIPEDA* does not expressly prohibit mere *attempts* to collect personal information. This is an obvious gap in the legislation that needs to be filled: attempts to collect, use or disclose personal information without consent should be covered by PIPEDA, even where they are unsuccessful.

¹⁶ *Morgan v. Alta Flights (Charters) Inc.*, 2006 FCA 121.

Recommendation #22:

Amend subs.4(1)(a) as follows: "This Part applies to every organization in respect of personal information that (a) the organization collects, uses, or discloses, or attempts to collect, use or disclose, in the course of commercial activities...."

State surveillance

As originally passed in 2001, PIPEDA was intended to maintain the *status quo* in terms of law enforcement collection of personal information from private enterprises. It thus permits organizations to disclose personal information to government institutions without judicial authorization (subs.7(3)(c.1) and (d)). However, the term "government institutions" in these provisions is neither defined nor qualified. In particular, it is not clearly limited to Canadian government institutions. Yet, many Canadians are concerned about the level of foreign outsourcing of information processing, and the powers of foreign agencies such as the FBI in the United States to access such data directly from private businesses upon demand, and under cover of secrecy, for "counter-terrorism" purposes (under the *USA Patriot Act*).

If these provisions were amended accordingly, foreign government requests for data about Canadians (other than subpoenas, warrants or orders made by bodies with jurisdiction to compel the production of the information) would have to go through Canadian government entities. Consideration should also be given to limiting subs.7(3)(c) re: subpoenas, court orders, etc. in this manner. This would be an appropriate and potentially effective safeguard against abusive foreign government practices.

Recommendation #23:

Amend subsections 7(3)(c.1) and (d) to make it clear that they apply to *Canadian* government institutions, not to foreign government institutions.

The *Public Safety Act* took subs.7(3)(c.1) a step further, amending PIPEDA so as to permit organizations to collect, as well as disclose, personal information for law enforcement purposes (subs.7(1)(e)). Many citizens are concerned about allowing private companies to act as agents of the state, as it points Canada in the direction of past societies such as Maoist China, communist Romania and East Germany that relied upon exactly such extensions of state power. Such a move shifts the balance of power between state and citizen in a way that places citizens at greater risk of harm from abuse of these new powers. It is not clear that such risk of state abuse in the future is outweighed by the benefits of the new powers in terms of protection of citizens from criminal activity.

Recommendation #24:

Repeal subs.7(1)(e) of PIPEDA.

Definition of “Organization”

PIPEDA defines “organization” as including “an association, a partnership, a person and a trade union”. This definition is remarkably unhelpful in determining whether corporate affiliates are separate organizations under PIPEDA, thus subject to separate consent requirements (such that information cannot be shared between them without proper consent from the individual). It should specify that affiliates are separate organizations for the purpose of PIPEDA.

Recommendation #25

Amend the definition of "organization" to "...includes an association, a partnership, a *related organization*, a person and a trade union."

Recommendations

Recommendation #1:

Give the Privacy Commissioner (or an associated Tribunal) order-making powers, similar to those of the Alberta and B.C. Commissioners.

Recommendation #2:

Should PIPEDA be amended to give the Commissioner discretion with respect to the investigation of complaints, it should be further amended to require that the Commissioner respond in writing to each complainant within 30 days of the complaint, setting out whether or not the complaint will be investigated. This would free complainants up to pursue the matter in court if the Commissioner chooses not to inquire into their complaints.

Recommendation #3:

If PIPEDA is amended to give the Commissioner order-making powers, include a statutory right of action for damages for successful complainant via an expedited procedure in Federal Court (or Tribunal), under which applicants are insulated from adverse costs orders and are entitled to solicitor-client costs should they succeed in obtaining damages.

If the current redress/enforcement regime is retained, amend s.14 of PIPEDA to protect bona fide applicants from adverse cost awards in Federal Court, and provide for solicitor-client costs in the event of successful applications.

Whether or not the redress/enforcement regime is changed, protect individual applicants for judicial review of Commissioner decisions from adverse cost awards other than in exceptional circumstances.

Recommendation #4:

Protect complainant privacy by requiring the Federal Court (or Tribunal) not to publish any identifying information about complainants in applications for damages, enforcement, judicial review, or otherwise.

Recommendation #5:

Provide for punitive as well as compensatory damages under s.16 of PIPEDA.

Recommendation #6:

Permit class actions under s.14 of the current model or under a new statutory right of action, if adopted. Further amend s.14 to permit Federal Court applications by similarly affected individuals, not just those complainants who lodged the complaint in question.

Recommendation #7:

Amend s. 20 of PIPEDA to require publication by the Commissioner of full decisions, including names of organizations, but not including identifying information about complainants.

Recommendation #8

Amend s.25 of PIPEDA to require specific annual reporting by the Commissioner on the type, treatment, and resolution of all complaints received. Such reporting should include the total number of complaints received, the number of complaints not investigated, the number of complaints for which resolution was attempted via mediation or conciliation, and the number that were ultimately decided by way of orders or findings.

Recommendation #9:

Expand s.28 of PIPEDA to cover willful violations of the Act, knowingly misleading the Commissioner, and (if the Commissioner or a Tribunal is granted order-making powers), failing to comply with such orders.

Recommendation #10:

Amend PIPEDA to explicitly permit the Commissioner to share information and cooperate in investigations with counterparts in other countries and in all provinces in Canada.

Recommendation #11:

Remove the "reasonable grounds" requirement for audits.

Recommendation #12:

Amend Principle 7 of PIPEDA to include a requirement to notify affected individuals of a security breach that results in the acquisition of unencrypted personal information by an unauthorized person. Such requirement should include specifics regarding the type of personal information and breach that triggers the obligation to notify, form and content of notices, timing of notices, who should be notified, etc.

Failure to notify affected individuals as required under the Act should be subject to tough penalties.

Recommendation #13:

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 "Organizations 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 #14

Amend the poorly drafted "refusal to deal" section in PIPEDA (Principle 4.3.3) to replace "...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 #15

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 #16

Include in Principle 4.4 of PIPEDA a requirement that personal information be collected directly from the individual unless the individual has consented to the 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 #17:

In Principle 4.3.1, replace the two last sentences "Typically, 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.”

Recommendation #18:

Amend s.1(a) of PIPEDA's Regulations specifying "publicly available" information (SOR/2001-7) to allow individuals to opt-out of secondary uses of their information published in the telephone directory.

Recommendation #19:

Amend subsection 5(3) to cover practices as well as purposes. Suggested drafting: "An organization may collect, use or disclose personal information only for purposes and only in a manner and to an extent that a reasonable person would consider are appropriate in the circumstances."

Alternatively, adopt the Alberta approach, under which both purposes and practices are subject to a "reasonableness" test (see ss.11(2), 16(2), 19(2), Alta PIPA).

Specify components of the "reasonableness" test as follows:

- (a) rational connection of the collection, use or disclosure to a reasonable purpose;
- (b) minimal impairment of the individual's privacy rights in achieving that purpose; and
- (c) proportionality as between the commercial purpose and the loss of individual privacy.

Include a new clause in subsection 5(3), setting out examples of inappropriate collection, use and disclosure. Suggested drafting: "For greater certainty, the following purposes and practices would not be considered appropriate by reasonable persons...."

Recommendation #20:

Include in PIPEDA specific rules limiting the collection, use and disclosure of children's personal information. Such rules should be at least as strict as those already adopted in the Canadian Code of Practice for Consumer Protection in Electronic Commerce and by the Canadian Marketing Association. There should be strict and significant penalties for violating these provisions.

Recommendation #21:

Amend Principle 4.8.2(e) to replace "related organizations" with "third parties, including related organizations".

Amend Principle 4.8 to include a new clause requiring disclosure of "sources other than the individual from which the organization obtains personal information."

Amend Principle 4.9.1 to replace "Organizations are encouraged to indicate the source of this information" with "Upon request and to the extent possible, organizations shall

disclose all sources from which they have obtained personal information about the individual."

Recommendation #22:

Amend subs.4(1)(a) as follows: "This Part applies to every organization in respect of personal information that (a) the organization collects, uses, or discloses, or attempts to collect, use or disclose, in the course of commercial activities...."

Recommendation #23:

Amend subsections 7(3)(c.1) and (d) to make it clear that they apply to Canadian government institutions, not to foreign government institutions.

Recommendation #24:

Repeal subs.7(1)(e) of PIPEDA.

Recommendation #25

Amend the definition of "organization" to "...includes an association, a partnership, a related organization, a person and a trade union."

