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

Comments in Response to the Privacy Commissioner of Canada's PIPEDA Review Discussion Document

September 7, 2006

Introduction

CIPPIC welcomes this opportunity to provide comments to the Privacy Commissioner of Canada on the *Personal Information Protection and Electronic Documents Act* ("PIPEDA"), with a view to the upcoming Parliamentary review of the Act. Our comments are the result of both extensive research and analysis conducted by CIPPIC students and CIPPIC associates, and the extensive involvement and experience of CIPPIC's Executive Director with PIPEDA and its predecessor, the CSA Code.

We are commenting on most, but not all, of the issues raised by in the Discussion Paper. We have also raised a few additional issues for consideration. This submission does not constitute an exhaustive list of issues, from our perspective, regarding PIPEDA. It does, however, raise most of the key issues that we think need to be considered in the PIPEDA review.

1. Commissioner's Powers

Is the existing ombudsman model effective or ineffective at protecting the privacy rights of individuals and addressing the legitimate interest in personal information of organizations engaged in commercial activities? In what ways? What, if anything, needs to be changed?

This, in CIPPIC's view, is the single most important issue for consideration in the PIPEDA review.

After five and a half years of experience with PIPEDA, it is clear that the current "ombudsman" model fails to provide adequate incentives for compliance, and that change of some kind is required if PIPEDA is to be effective. What form such change should take is debatable, especially since not all powers at the disposal of the Office of the Privacy Commissioner ("OPC") have been used.

CIPPIC advocates increased use of certain existing powers (including "naming and shaming", auditing, and public education) by the OPC, as well as the granting of order-making powers to the OPC, consistent with the three provincial privacy commissioners overseeing private sector data protection laws. Combining elements of the ombudsman approach with order-making powers is neither impossible nor inadvisable. Indeed, it is currently being done with good results in other jurisdictions.

The current approach is not working

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.

While almost all companies we assessed had a privacy policy and were thus aware of the need to respect customer privacy, many failed to fulfill even basic statutory requirements, such as providing contact information for their privacy officers, clearly stating what they do with consumers' personal information, and responding to access to information requests. A significant proportion of the policies we examined were unclear on key points such as whether or not consumer information is shared with other companies. Many failed to provide a clear and conspicuous method for consumers to opt-out of unnecessary uses and disclosures of their personal information, often relying on a clause buried deep in a lengthy privacy policy that consumers are unlikely to review.

A number of policies we examined were misleading, suggesting for example that no secondary use or sharing of personal information would take place without the consumer's explicit consent, but then assuming such consent unless the consumer exercised an often inconspicuous or incomplete opt-out.

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

---

[1] *Compliance with Canadian Data Protection Laws: Are Retailers Measuring Up?* (CIPPIC, May 2006) was funded in part by the Office of the Privacy Commissioner and the Social Sciences and Humanities Research Council. The report can be accessed from www.cippic.ca and is available in hard copy for a fee.
[2] BCCLA, *Securing Compliance, Protecting Privacy: The PIPEDA Enforcement Evaluation Project* (March 2006), p.83.
[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).

A strict "ombuds" model is inappropriate for government 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" (the controversial "naming and shaming" power), 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.

As the Privacy Commissioner has noted,[6] 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) ombudsman 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, whether through the use of publicity or through order-making powers.

The pure ombuds approach focusing on individual complaint resolution in confidence is particularly unsuitable in the case of new legislation, where industry education is critical, given the prior existence of non-compliant industry practices. In such a context, industry needs clear and useful guidance in the form of detailed findings, advance rulings, and interpretation bulletins. Dispute resolution should be a lower priority for the OPC, although individuals should have access to some low cost, efficient and effective means of obtaining redress for privacy violations.

[6] "*Cherry-picking among apples and oranges: refocusing current debate about the merits of the ombuds-model under PIPEDA",* (Toronto: Oct.21, 2005)

Strong coercive and 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.[7] 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. As the BCCLA concludes in its comparative review of enforcement powers:

> "that all three provinces are apparently able to work within a conciliation model while retaining coercive powers not granted under PIPEDA may be a telling rejoinder to the claim that, for example, order-making power would negatively impact the ability of the federal OPC to successfully resolve disputes through mediation and/or conciliation."[8]

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."[9] 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.

The Commissioner should exercise all of her existing powers under PIPEDA

It is difficult to judge whether the compliance problem under PIPEA is a result primarily of flawed legislation (in particular, the Commissioner's inability to make enforceable orders) or of a failure by the Commissioner to use all of the powers available to her. In any case, it is CIPPIC's view that the Commissioner should take a more proactive approach to exercising her powers under PIPEDA.

Publicity: naming complaint respondents

PIPEDA provides the Commissioner with substantial powers of enforcement through the use of publicity. Section 20 of the Act states:

---

[7] Ibid.; OPC Discussion Document
[8] *Op cit*, p.50.
[9] Ibid, p.41.

> **20.** (1) Subject to subsections (2) to (5), 13(3) and 19(1), the Commissioner or any person acting on behalf or under the direction of the Commissioner shall not disclose any information that comes to their knowledge as a result of the performance or exercise of any of the Commissioner's duties or powers under this Part.
>
> (2) The Commissioner may make public any information relating to the personal information management practices of an organization if the Commissioner considers that it is in the public interest to do so.

We understand that the current Commissioner interprets these two provisions together as not permitting publication of complaint respondent names as a matter of course. We, like others, respectfully disagree with this interpretation. If the Commissioner considers it in the public interest to name complaint respondents routinely, she is empowered to do so. In any case, there is agreement that this power should be used in cases of repeated or ongoing non-compliance. However, we have yet to see it being used.

It is noteworthy that the Alberta Privacy Commissioner's office, which makes a practice of naming respondents in detailed public findings, "believes that the ability and willingness to name names, in appropriate circumstances, is a powerful tool for achieving compliance."[10]

Bad publicity is often far more costly to an organization than is a financial penalty. Yet, the Commissioner has chosen not to employ this tool other than in cases where the matter was already public. This policy of not naming complaint respondents, together with the lack of order-making powers on the part of the Commissioner, leaves organizations with little incentive to comply, at least until they are "caught out": the cost of non-compliance is merely a confidential investigation and recommendation by the OPC, and possibly even a pat on the back for changing a policy that should have been changed years ago.

There are good arguments both for naming complaint respondents as a matter of course, and for saving this power for use only in cases of non-compliance, or possibly egregious or repeated non-compliance. The former approach would provide much needed transparency and guidance to industry and the public, by creating a body of contextual findings rather than the sanitized, anonymous findings now published. As more companies are named, the associated stigma would likely decline, reducing the deterrence effect of publicity. The latter approach would increase the stigma of being named, and might thus be an effective deterrence measure. However, it would fail to deter those companies who delay compliance until caught, and would offer little additional guidance to industry than currently is the case.

For this reason, in the absence of other effective compliance tools, we advocate routine naming of organizations found by the OPC to have violated the Act. Exceptions can be made for *bona fide* errors or other unusual circumstances in which it would be unfair to

[10] as cited in BCCLA, *op cit*, p.39.

single out the particular company. We doubt that the naming of repeat or ongoing offenders will, on its own, achieve significantly greater compliance than is currently the case.

Performing audits

PIPEDA also provides the Commissioner with the power to audit organizations, if she "has reasonable grounds to believe that the organization has been contravening [the Act]".[11] 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. Surprisingly, this potentially powerful compliance tool remains, to our knowledge, yet to be employed, although the OPC has indicated its intention to use it. Apparently, a key stumbling block from the OPC's perspective is the "reasonable grounds" requirement. Like the public interest test for naming complaint respondents, the "reasonable grounds" test in s.18 is subject to varying interpretations. And like its approach to naming respondents, the OPC seems to be taking an excessively conservative approach to its audit power. We submit that there are numerous cases in which reasonable grounds for an audit exist, and for which an audit would be highly beneficial for the purpose of educating industry and encouraging compliance. We are concerned that this important power remains unused, and advocate much more aggressive use of it.

Nevertheless, 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. It is highly unlikely that such a power would be abused, given its cost to the OPC. Indeed, it is unlikely that the OPC would exercise this power without reasonable grounds. However, making reasonable grounds a prerequisite for audits has apparently proven to be a serious roadblock in the exercise of this important power. For this reason, we advocate removing the "reasonable grounds" requirement in section 18.

Investigating complaints

As noted above, the Commissioner has strong investigatory powers, comparable to those of the Competition Bureau and other regulatory agencies. These powers include, under s.12, summoning witnesses, entering premises, and examining and copying records found on premises. Not explicitly mentioned in the list of powers is the right of the Commissioner to test respondent policies and practices by, for example, covertly engaging in transactions with respondents, or to collect and use personal information about individuals without their knowledge or consent for the purpose of an investigation (a practice that PIPEDA explicitly permits under subs.7(1)(b) and 7(2)(d)).

CIPPIC takes the position that such powers are implicit in the legislation. However, in response to a complaint we lodged against an online American databroker that sells data about Canadians to Canadians, the OPC concluded that it "cannot proceed with your complaint as we lack jurisdiction to compel U.S. organizations to produce the evidence

[11] subs.18(1)

necessary for us to conduct the investigation".[12] Implicit in this finding is a determination that the only way to investigate the alleged practices of an online data broker is by compelling the respondent to provide evidence of Canadian sources. CIPPIC respectfully disagrees with this determination, and is challenging it in Federal Court by way of an application for judicial review. Although we expect the Court to clarify the scope of the Commissioner's investigatory powers, it could be helpful for the legislation to include among the Commissioner's investigatory powers, the power to collect and use personal information without consent for investigatory purposes, and the power to engage covertly in transactions for investigatory purposes.

Publishing Findings

The OPC has made a practice of publishing its findings, although only in summary form and, increasingly, only for selected cases (e.g., where new issues are raised). This practice has provided the industry and interested public with significant guidance on the many grey areas of PIPEDA. However, such guidance has been limited by the summary nature of the findings as well as by the decision not to name respondents. More useful from an educational perspective would be the publication of possibly fewer but definitely more detailed case findings, in which respondents are named and the facts are thoroughly set out. All significant findings should be so published, with a view to educating industry and establishing a useful "jurisprudence" for future reference. The Alberta approach in this respect is a useful model to consider.

The "reasonable grounds" prerequisite for audits should be removed

See above, under "Performing Audits". Although we believe that the Commissioner can and should be much more aggressive in her use of this power as drafted, the "reasonable grounds" requirement appears to be causing unnecessary and counter-productive reticence on the part of the OPC to exercise this power. For the reasons stated above, we recommend removing this prerequisite for audits, altogether.

"Watchdog" complaints should continue to be allowed

Recognizing that many privacy invasions, by their very nature, go unnoticed by affected individuals, and that there is therefore a need for "watchdogs" to act on behalf of the public in holding organizations accountable for their data practices, PIPEDA permits any individual to complain about an alleged breach, without having to prove damages or establish a direct interest in the particular breach. This is a critically important and beneficial aspect of the current complaints-based regime. It should be retained.

Some of the most useful findings generated by the OPC have been those in response to watchdog complaints. This is not surprising given that such complaints tend to be about ongoing practices and important policy issues rather than one-time breaches due to

[12] letter to CIPPIC dated November 18, 2005 re: Abika.com; <http://www.privcom.gc.ca/legislation/let/let_051118_e.asp>

human error or oversight. If watchdog complaints were not permitted, many important privacy issues and widespread PIPEDA violations might never be investigated.

Complainants should not be required to attempt resolution with the organization as a matter of course

In keeping with the approach to watchdog complaints described above, it would be inappropriate to require complainants to first attempt resolution of the issue with the organization in question. Many complaints raise difficult policy issues and/or involve industry-wide practices. These are not so much disputes between two parties as they are matters of policy that need to be examined and ruled upon by an authority. The current legislative regime permits the Commissioner to demand, in appropriate cases, that complainants first attempt resolution with the organization, but it does not require such attempts where inappropriate. This approach should be maintained.

The legislation should provide for punitive damages.

Under s.16 of the Act, the Federal Court is empowered to "award damages to the complainant, including damages for any humiliation that the complainant has suffered". Punitive damages are not specified as a possible remedy, although like damages for humiliation, they are part of the Court's general arsenal of remedies.

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".[13] In the context of privacy breaches, quantifiable damages are often minimal even though the violation may be egregious. Punitive damages in this context may be the only meaningful remedy for complainants. Without the possibility of punitive damages, even the most meritorious and compelling cases may not be brought, simply because of the difficulty proving damages or the potentially low dollar awards for privacy breaches.

Whatever body is empowered to make binding orders under PIPEDA should also have the power to order punitive as well as compensatory damages. Although the Federal Court already has this power, specifying it along with the power to award general damages would make sense. The Commissioner or a new Tribunal would require explicit powers to award punitive damages.

Class actions should be allowed

Privacy invasions in the course of commercial activities often affect many individuals at once. A company that routinely discloses its customer data to third parties without consent, for example, is violating the privacy rights of all its customers. Yet, PIPEDA's enforcement regime is designed to serve only individual complainants. Under s.12, only "an individual" may file a complaint. As a result, CIPPIC has been asked by the OPC to limit complainants on any one complaint to a single person – an unnecessary and

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

inappropriate restriction, especially given that many people may have been similarly affected by a given breach. Under s.14, only that individual complainant may apply to court in order to obtain a binding ruling. Thus, although a given complaint may affect hundreds of individuals, only the individual who lodged the complaint can subsequently take it to court and obtain redress for him or herself. Other similarly affected individuals are foreclosed from seeking redress in the court, unless they launch their own complaint with the OPC.

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 where individual actions would not proceed or where even successful individual actions would make no difference to the company's practice.

PIPEDA should be amended to allow for class actions. This can be done in two ways:

(1) via a statutory right of action for breach of PIPEDA by representative plaintiffs, regardless of whether or not they have filed a complaint with the OPC. Representative plaintiffs should be permitted to exercise such a right in any court, not just Federal Court. Class actions would then be possible in all courts permitting them, providing plaintiffs with more options in terms of legal representation.

(2) allow representative complaints by individuals under s.11, and amend s.14 to clarify that a complainant can proceed to Federal Court on behalf of others and by way of action or application.

In either case, in order to make class actions for privacy breaches practicable, the statute should also allow for punitive damages and solicitor/client costs in the event that a breach is found.

The Commission (or a related Tribunal) should have the power to issue binding orders

A feature of the current regime that surprises many people is that the Commissioner, unlike her counterparts in other provinces, has no power to issue binding orders. Nor is there a specialized tribunal (such as the Human Rights Tribunal) to which she can refer complaints for binding resolution. As a result, complainants have no low-cost, easy method by which to vindicate their rights and hold corporations accountable under the law, when the ombuds approach fails. They must apply to Federal Court for a hearing *di novo* – an extremely costly (and risky) process that, for most complainants, requires legal representation.

Moreover, the lack of OPC order-making powers under the current regime forces complainants to make their case twice in order to obtain a legally binding ruling: first to the OPC, and then to Federal Court. This two-stage process is unnecessarily protracted, as the OPC may take up to a year to investigate and report on the complaint, and has in fact been taking longer in a number of instances. By the time a matter gets to court for binding resolution, it may be moot.

Providing the Commissioner with order-making powers, either directly or via registration of orders in Federal Court, would significantly strengthen the enforcement regime under PIPEDA. It would also vest order-making powers in an expert body that is better equipped than a generalist body (e.g. Federal Court) to rule on matters of data protection. It would, of course, require a significant change of approach on the part of the OPC. However, it is clear that significant changes are needed if PIPEDA is to be effective.

An alternative that should be considered is the establishment of a specialized tribunal to which the Commissioner and/or complainants can submit complaints for binding resolution. This approach has the attraction of clearly separating ombuds functions (Commissioner) from adjudicatory functions (Tribunal). In order to be effective, however, the tribunal must be accessible to complainants and the interested public at minimal cost (e.g., no legal representation required)

In either case, the legislation should provide for a right of appeal to Federal Court.

The Commissioner (or Tribunal) should be empowered to award compensation to complainants, as well as punitive damages against respondents.

Regardless of whether the Commissioner (or a new Tribunal) is given order-making powers, she should be empowered to award compensation to complainants.

Currently, complainants who have suffered damages as a result of a breach of PIPEDA must sue in Federal Court in order to force recalcitrant respondents to compensate them. While most such cases are eventually settled, it is often the lodging of a formal lawsuit that forces the settlement. Moreover, complainants frequently settle for much less than they feel is fair, simply because of the cost of litigation. Empowering the Commissioner to award compensation to complainants would likely improve compliance while offering individuals better access to remedial justice.

For the same reasons as set out above, the Commissioner should be empowered to award punitive damages in addition to compensatory damages.

2. Consent:

(a) Employer/Employee

Should PIPEDA be amended to remove the consent requirements in relation to personal employee information? If so, is the "reasonable purpose" test an appropriate alternative?

No, the general rule of consent should apply to employees as well as to consumers. While it is true that consent is not always meaningful given the tremendous imbalance of power in the employment relationship, similar imbalances exist in the consumer context. Moreover, the consent requirement serves to ensure that employees are at least given notice of the data collection, use or disclosure in question. And in some cases, employees will exercise their rights to refuse consent.

The "reasonable purpose" test in subs.5(3) is not a substitute for consent. Rather, it complements the consent requirement by ensuring that, regardless of consent, the data is not being collected, used or disclosed for an inappropriate purpose. This is a critical element of employee data protection, but it does not substitute for notice and consent.

Should employee consent issues be addressed by a specific exception in section 7 for the employment relationship, subject to conditions? If so, what should be the conditions?

Yes, this is the appropriate way to deal with employment-specific exceptions to the normal rule of consent. Conditions should include a requirement for notice, except where inappropriate. Employees should, for example, be informed up front of any employer monitoring or background checks. Covert collection of information about employees should be permitted only where justified on the basis of reasonable suspicion of wrongdoing. Other conditions should include necessity: the information collection, use or disclosure should be necessary for the purposes of establishing, managing or terminating an employment relationship.

(b) Law Enforcement and National Security

Is it appropriate for private sector organizations to act as personal information collection agents for the government? Is it appropriate for records to be created solely for the purpose of providing them to government?

No, it is not appropriate for private sector organizations to act as agents for the government in its law enforcement activities. CIPPIC opposes the *Public Safety Act* amendments to PIPEDA for this reason.

PIPEDA, as originally passed by Parliament, was carefully drafted so as to maintain the status quo regarding private sector involvement in law enforcement, drawing the line at

voluntary or responsive disclosures of personal information already collected for other purposes (subss.7(3)(d) and 7(3)(c.1)). Even subs.7(3)(c.1), which allows private organizations to disclose personal information in response to warrantless requests by law enforcement or government bodies, is highly controversial and opposed by many Canadians on the grounds that it breaches the fundamental principle that searches should only be conducted with prior judicial authorization. Yet this provision merely allows for disclosures; it does not permit private entities to proactively collect personal data for the purpose of law enforcement. Nor should it.

Law enforcement agencies have a very important mandate and broad powers with which to exercise it. Because those powers are vulnerable to abuse, free and democratic societies have built up a number of safeguards designed to prevent such abuses. Such safeguards include the requirement to obtain warrants for non-consensual searches and various oversight mechanisms designed to constrain intrusive state activities. By permitting private organizations not only to disclose but also to *collect* personal information without warrants, in order to then disclose to law enforcement agencies, PIPEDA has put private organizations in the position of acting as agents of the state, without corresponding oversight mechanisms. The *Public Safety Act* amendments seek to circumvent these carefully constructed safeguards aimed at protecting the civil liberties of Canadians. For this reason, they should be rescinded.

Is the authority to collect personal information without the knowledge or consent of the individual in section 7(1)(e) broader than necessary? If so, how might the provision be amended to limit the authority for organizations subject to PIPEDA to collect information?

Yes, the provision is much broader than necessary. Indeed, for the reasons set out about, it is inappropriate and should be rescinded in its entirety.

In the absence of such rescission, it should at least be amended to limit the amount of information that can be collected, the duration of collection activity, and the sources from which the information can be collected. If the aim of this new provision was to permit certain types of organizations to collect certain types of information for future delivery to law enforcement agencies, the provision should be narrowly drafted to achieve this goal and this goal only.

(c) Investigative Bodies

Should provisions in PIPEDA relating to investigative bodies be changed? If so, in what way?

No. CIPPIC supports the current approach to investigative bodies under PIPEDA. While it may entail some administrative cost to investigative bodies and government, the current approach of listing investigative bodies in a regulation provides a valuable level of transparency to the public (given the exceptions for investigative bodies under PIPEDA)

as well as a mechanism (the application/approval process) that does not rely on self-designation by entities with a vested interest in such designation.

The Alberta and B.C. approaches to investigative bodies create a lower threshold for protection of personal information, both procedurally, by allowing organizations to collect, use and disclose personal information for the purposes of an investigation, and substantively, by defining "investigation" more broadly than in the case of PIPEDA's investigatory body exceptions, which are limited to disclosures related to contravention of laws or breach of an agreement. Thus, organizations in Alberta and B.C. need not be designated as "investigative bodies" in order to collect, use or disclose data without consent. Moreover, the scope of circumstances in which they can engage in non-consensual practices is broader than under PIPEDA.

CIPPIC appreciates the administrative burden associated with the current regime, and has researched the matter in some depth, with a view to identifying solutions that would ease the burden for industry and government while still offering substantial privacy protection to individuals. We have been unable to identify an alternative approach that achieves these dual goals. Providing general exceptions for "investigations", as in Alberta and B.C., inevitably lowers the standard of protection, for the reasons set out above.

Whether the provisions are changed or not, can the transparency and accountability relating to the activities of investigative bodies be further enhanced? What measures would accomplish this?

Yes. We recommend the following measures:

1. Industry Canada should provide better clarity in the RIAS as to what information will be required in an application versus what are the specific evaluation criteria. The criteria applied by Industry Canada should be specifically enumerated in a public document.

2. PIPEDA should not permit specification of investigative bodies by class, and the regulation should eliminate listings by class (i.e., paragraphs (w) and (x), which exempt licensed private investigators and insurance adjusters).

3. All professional associations that qualify member organizations as investigative bodies should apply individually, and upon approval from IC, be listed by name. Such association level applications would be subject to additional qualification criteria including:
    a. the association must analyze and verify the privacy policy of any member organization requesting inclusion under its listing;
    b. the association must maintain a current and easily accessible database of all members qualifying as "investigative bodies"; and
    c. the association must include in its constitution procedures for monitoring and reviewing the compliance of its qualified members to their privacy

codes, and for the removal of qualification from members who fail to comply.

(d) Attempted Collection without consent

Should* PIPEDA *be amended to regulate willful attempts to collect personal information without consent?

Yes, PIPEDA should be amended to apply to willful attempts to collect personal information without consent, as well as to actual collection without consent. As noted in the discussion paper, a recent Federal Court case highlighted this gap in PIPEDA. Attempts to collect personal data in breach of the Act should be constrained in the same way that actual violations are.

(e) Individual, Family and Public Interest Exceptions

Are there circumstances beyond those now identified in section 7 of* PIPEDA *where collection, use or disclosure without knowledge or consent should be permitted for the legitimate benefit of an individual or his or her family or the greater public? If so, what are those circumstances?

CIPPIC has no comment on this issue at this time.

(f) Blanket consent

Should* PIPEDA *be amended to deal with "blanket consent?" If so, what should be the nature of those amendments?

CIPPIC is in strong agreement with the view expressed in the Discussion paper that "truly free and informed consent is more than this; it is more than a one-time, wide-open, blanket signature on a consent form. They may argue that informed consent is a dynamic process that involves keeping individuals actively aware – on an ongoing basis, using understandable language, and in a transparent manner – of what an organization intends to do with their personal information and for what purpose". "Blanket consent" is a widespread and serious problem for data protection, as it subverts the intent of the legislation and renders the concept of consent effectively meaningless.

While there are some amendments to PIPEDA that would help in this respect (see below), the problem of "blanket consent" can and should be addressed through Commissioner and Court interpretations of the statute. PIPEDA includes many provisions designed precisely to prevent overly broad and vague consent clauses. Such provisions include:

> 4.3.2: … Organizations shall make a *reasonable effort* to ensure that the individual is advised of the purposes for which the information will be used. To make the consent meaningful, the purposes must be stated in such a manner that the individual *can reasonably understand* how the information will be used or disclosed. [emphasis added]
>
> 4.8.1: Organizations shall be open about their policies and practices with respect to the management of personal information. Individuals shall be able to acquire information about an organization's policies and practices *without unreasonable effort.* This information shall be made available in a form that is *generally understandable.* [emphasis added]
>
> 4.8.2: The information made available shall include
> (a) the name or title, and the address, of the person who is accountable for the organization's policies and practices and to whom complaints or inquiries can be forwarded;
> (b) the means of gaining access to personal information held by the organization;
> (c) a description of the type of personal information held by the organization, including a general account of its use;
> (d) a copy of any brochures or other information that explain the organization's policies, standards, or codes; and
> (e) what personal information is made available to related organizations (e.g. subsidiaries).

Principles 4.3.2 and 4.8.1 set admittedly vague standards for the communication by organizations to individuals of their data practices (e.g., "reasonable steps", "unreasonable effort", "generally understandable"). However, these provisions can (and should) be interpreted as requiring more than "blanket consent" to an undefined set of data practices. It is up to the Commissioner (and Federal Court) to interpret and apply these provisions in relevant cases, and to thereby signal to businesses that "blanket consent" is not acceptable.

Nevertheless, it would be helpful for the legislation to provide clearer guidance on this issue. Principle 4.8.2 does so to an extent, but leaves some gaping holes. In particular, Principle 4.8.2 should be amended to require that organizations make available information about:
a) the sources from which they collect personal data, [14]
b) the names and/or types of organizations with whom they share personal data, and
c) the type of personal data they share with any other organizations (not just related organizations, as currently stated in 4.8.2(e)).

Based on the results of CIPPIC's recent PIPEDA compliance study, most organizations share customer information with unrelated third parties. Many do not have affiliates. By limiting the explicit notice requirement in 4.8.2(e) to related organizations, PIPEDA

[14] This amendment should also be made to Principle 4.9.1: organizations should be required, not just encouraged, to indicate the source of personal data when asked.

suggests that explicit notice regarding disclosures to unaffiliated third parties is not required. In any case, the limited scope of this disclosure requirement makes no sense; organizations should be required to give consumers clear notice of all personal information disclosures they make to third parties. They should also be required to name the organizations, or at least identity the types of organizations, with which they share data.

Another problem associated with "blanket consent" is temporal: other than in the case of data retention (Principle 4.5), PIPEDA sets no limits on the time period for which consent is valid. Yet, there are likely to be cases in which it will be unreasonable for an organization to continue to assume consent, given, for example, the elapse of several years without contact with the individual. This problem may be best addressed through a general reasonableness requirement rather than a set time period.

Other consent-related issues

(g) Clarifying forms of consent and associated requirements

Principle 4.3.4 allows for the form of consent sought by an organization to vary, but PIPEDA (unlike the Alberta and B.C. Acts) does not distinguish between express, implied, and opt-out consent, and provides no prerequisites or criteria for reliance on each type of consent. While the Privacy Commissioner has published guidelines for determining the appropriate form of consent,[15] the findings from CIPPIC's recent PIPEDA Compliance study demonstrate that this is not sufficient: some organizations lack even a basic understanding of the differences between opt-in and opt-out consent, not to mention the appropriate use of opt-out methods.

Confusion has resulted from the use of the term "implied consent" to cover not only situations in which consent is *actually* provided (i.e., where the person would have consented if asked, and where the facts clearly suggest that consent was provided), but also situations in which consent is merely *deemed* (i.e., where it cannot reasonably be determined that the person would have consented if asked).

There is an important difference between "implied consent" and "deemed consent". In the former, the individual has actually consented; whether consent can be implied is a matter of fact, not of law. In the latter, it does not matter whether the individual has actually consented; the law permits organizations to act as if the individual has consented.

This difference is important insofar as it leads to differing standards of notice in each case. Notice is of less importance in the situation where consent can be implied. This is because consent can only be implied where it is reasonable to assume that the individual is fully aware of the collection, use, or disclosure and agrees to it. On the other hand, notice is of critical importance in those situations where consent is deemed, since the

[15] "Determining the appropriate form of consent under the *Personal Information Protection and Electronic Documents Act*", <http://www.privcom.gc.ca/fs-fi/02_05_d_24_e.asp>

onus is then on the individual to "opt out" if he or she desires (or, in cases where no opt-out is offered, the individual needs at least to be aware of the uses to which the individual's information will be put).

Negative option consent, the most prevalent form of consent for use of personal data in the marketplace, is a form of "deemed consent", since it deems consent regardless of whether the individual is actually aware of the use, let alone consents to it. A test for validity of negative option consent has emerged through Commissioner findings. While this is helpful, incorporating this test into the legislation would be even better.

CIPPIC recommends, therefore, that PIPEDA be revised so as to clearly define and distinguish between these different forms of consent, applying different criteria and standards of notice to each, as appropriate. The Alberta and B.C. Acts provide useful models, improving substantially on PIPEDA in this respect.

(h) Limiting collection, use, retention and disclosure

PIPEDA contains a number of "bottom line" protections that apply, regardless of consent, to limit private sector data practices.

Subs.5(3) of PIPEDA limits the purposes for which organizations can legitimately collect, use or disclose personal information to those "that a reasonable person would consider are appropriate in the circumstances". This "purpose limitation" clause has been relied upon in numerous PIPEDA findings and has served to provide a much-needed data protection "bottom line" in an otherwise largely consent-based regime. However, it merely limits the *purposes* for which organizations can collect, use or disclose personal information. It does not, strictly speaking, limit the *practices* of organizations – e.g., the extent of data collected or disclosed, the type of data collected or disclosed, or the source from which data is collected. Yet, in most cases, it is the organization's practice that is in question, not its purpose.

Other provisions in Schedule 1 of PIPEDA do go some way towards filling this gap. In particular, regardless of consent:

- Principle 4.4 limits collection to "that which is necessary for the purposes identified" – a necessity test;
- Principle 4.5 limits use and disclosure to purposes for which the information was collected, except with consent or required by law – a "rational connection" test;
- Principle 4.5 also limits retention for "only as long as necessary for the fulfillment of those purposes"; and
- Principle 4.3.3 limits the right of organizations to require consent except where "required to fulfil the explicitly specified, and legitimate purposes" – another necessity test.

These provisions add to subs.5(3)'s "bottom line" data protection to Canadians, but leave open the possibility of excessive use and disclosure and other inappropriate practices that

are nevertheless rationally connected to a legitimate and reasonable purpose. As a result, the Privacy Commissioner and Federal Court have had to read in to the Act protections against excessive disclosure and other inappropriate practices, particularly in cases where consent is not required (i.e., where an exception under s.7 applies). In a number of cases, the purpose limitation in subs.5(3) has been interpreted as a limitation on practices as well as purposes,[16] and in one recent finding, the Commissioner resorted to the purpose clause in s.3 to engage in a proper balancing analysis when faced with issues involving inappropriate practices *per se*.[17]

Such balancing typically involves a multi-step analysis, similar to that enunciated by the Supreme Court of Canada in the *Oakes* case, in order to determine whether a given practice would be considered, by a reasonable person, appropriate in the circumstances. In *Oakes*, the Court established a now oft-cited and applied test for justifying state limits on *Charter* rights:

> Two central criteria must be satisfied to establish that a limit [on *Charter* rights] is reasonable and demonstrably justified in a free and democratic society. First, the objective to be served by the measures limiting a Charter right must be sufficiently important to warrant overriding a constitutionally protected right or freedom. The standard must be high to ensure that trivial objectives or those discordant with the principles of a free and democratic society do not gain protection. At a minimum, an objective must relate to societal concerns which are pressing and substantial in a free and democratic society before it can be characterized as sufficiently important. Second, the party invoking s. 1 must show the means to be reasonable and demonstrably justified. This involves a form of proportionality test involving three important components. To begin, the measures must be fair and not arbitrary, carefully designed to achieve the objective in question and rationally connected to that objective. In addition, the means should impair the right in question as little as possible. Lastly, there must be a proportionality between the effects of the limiting measure and the objective -- the more severe the deleterious effects of a measure, the more important the objective must be.

The Commissioner and Courts have, in effect, been applying an *Oakes*-type test (appropriate purpose, rational connection, minimal impairment, and proportionality) to impugned data collection, use and disclosure practices under *PIPEDA*. Most notably, in a case involving workplace surveillance,[18] the Federal Court adopted the Commissioner's four-part test to determine whether the purpose in question was one that a reasonable person would consider appropriate in the circumstances:

- Is camera surveillance and recording necessary to meet a specific CP need?
- Is camera surveillance and recording likely to be effective in meeting that need?

[16] PIPEDA Case Summaries #317, 282, 130, 245, 232.
[17] PIPEDA Case Summary #279
[18] *Eastmond v. Canadian Pacific Railway*, 2004 FC 852 (CanLii).

- Is the loss of privacy proportional to the benefit gained?
- Is there a less privacy-invasive way of achieving the same end?

This approach makes sense. It is not sufficient that purposes be appropriate, and that practices be rationally connected to such purposes. *Practices* should also impair individual privacy as little as possible, and their privacy-invasive effects should be proportional to the importance of their purposes. But rather than forcing the Commissioner and Court to read in to PIPEDA a test that is not explicit but that is logically necessary for the integrity of the legislative regime (at least in the case of non-consensual collection, use or disclosure), the statute should make explicit such a test in a simple, clear manner.

CIPPIC therefore recommends amending subs.5(3) to reflect the full balancing test that the Commissioner and Court have developed in their interpretation of PIPEDA. In other words, this provision should be expanded to cover the practices themselves as well as their purposes. This could be done simply by adding the phrase "and only in a manner and to an extent" to the existing provision so that it reads:

> 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.

If subs.5(3) is not expanded to deal with excessive disclosures and other inappropriate practices, then at a minimum:

- a new clause should be added to s.7 so as to ensure that all non-consensual collection, use and disclosure is subject to an *Oakes*-type test of reasonableness;
- a new provision should be added, requiring that non-personal information be collected, used, or disclosed instead of personal information, as long as it will serve the specified purpose;
- a new provision should be added requiring that personal information be collected directly from the individual to whom it pertains, subject to certain listed exceptions; and
- consideration should be given to prohibiting the willful or reckless collection, use or disclosure of children's information (see below, under "Other Issues").

(i) Separating knowledge (notice) and consent

A separate Notice requirement

The "knowledge and consent" provision set out in Principle 4.3.2 combines two important concepts that warrant separate attention in the statute: notice and consent. As with consent, PIPEDA does not set out specific criteria for notice. In its study of business practices, CIPPIC found a number of instances in which companies provide consumers with a clear and conspicuous opt-out during the ordering process, but no clear notice of the secondary uses and disclosures in which the company engages. The

Commissioner's findings regarding the prerequisites for valid opt-out consent are helpful in this regard, but they would be more helpful if set out in the statute and applied to notice as well as consent.

We also found a wide range of practices with respect to notice – from clauses hidden in privacy policies to notices that consumers must read and respond to in order to complete an order. While the former is clearly inadequate and the latter is clearly adequate, it is not clear from PIPEDA where the line should be drawn. Setting out a separate requirement for notice with specific criteria would no doubt help companies ensure that their notice meets statutory requirements.

Requiring notice even where consent is not required

Following the CSA Code's approach of combining knowledge and consent, PIPEDA 's exceptions in section 7 apply to both knowledge and consent. Some exceptions specifically require notice, but others do not. It is not clear why some of the latter (e.g., disclosures for the purposes of collecting a debt, disclosures in response to subpoenas) do not include a notice requirement. CIPPIC recommends that all exceptions in s.7 include a notice requirement unless inappropriate or impracticable.

(j) Timeliness of consent

Principle 4.3.1 addresses the issue of *when* consent should be obtained, as follows:

> Typically, an organization will seek consent for the use or disclosure of the information at the time of collection. In certain circumstances, consent with respect to use or disclosure may be sought after the information has been collected but before use (for example, when an organization wants to use information for a purpose not previously identified).

This provision is remarkably unhelpful. It should be amended to require that consent be obtained at or before the time of collection, unless impossible or with respect to a purpose not previously identified.

(k) Refusal to deal

Principle 4.3.3 is another poorly drafted provision that has required the use of creative interpretation in order to achieve its intended objective. Not surprisingly, both Alberta and B.C. redrafted this provision in a more straightforward and sensible way. The PIPEDA version reads:

> 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 fulfil the explicitly specified, and legitimate purposes.

The Alberta version reads:

> An organization shall not, as a condition of supplying a product or service, require an individual to consent to the collection, use or disclosure of personal information about an individual beyond what is necessary to provide the product or service.

Principle 4.3.3 should be redrafted in the same way as the Alberta provision.

3. Disclosure of Personal Information before Transfer of Business

Should PIPEDA allow an organization in possession of personal information to disclose that information to a prospective purchaser or business partner? If so, what conditions should apply?

Yes, but only under strict conditions of confidentiality and subsequent destruction or return of the information if the transaction does not materialize.

Should PIPEDA be amended to allow the transfer of personal information from an organization to a business purchaser or business partner? If so, what restrictions should apply?

Yes, but again only on condition that (a) all individuals whose personal information is being transferred are notified of the transfer as soon as reasonably possible after the transfer, (b) the new owner or partner adheres to the organization's current policies respecting data privacy, and (c) no changes are made to the privacy policy within 60 days of the transfer.

4. Duty to Notify Individuals in event of Loss or Theft

Should organizations that suffer loss or theft of personal information have a legal duty to report the loss or theft? If so, under what conditions, and to whom should they report?

PIPEDA should incorporate a Legal Duty to Notify

CIPPIC recommends that PIPEDA be amended to require organizations to report the loss or theft of personal information they collect or store. This duty should be mandatory and should apply to all instances of security breaches, even where it is determined the threat of misuse, abuse or fraud is minimal. The underlying presumption would be that those potentially affected by security breaches of personal information ought to be notified as a matter of right.

The personal information of Canadians is being collected to an increasing degree, by many types of public and private organizations and not always with the knowledge or consent of the individuals concerned. With advances in technology, this practice can be expected to continue to increase and with it, so too will the risk of unauthorized access and identity theft.

All organizations are susceptible to security breaches and no currently used security measures, however sophisticated, provide total protection against unauthorized access to personal information, whether this access be accidental or fraudulent. In both instances, identity theft can result from the loss or theft, leading to a range of negative consequences for those affected.

For these individuals, not to be notified of security breaches borders on the unconscionable. They have a right to know if their personal information is in the hands of unauthorized persons or organizations and of the associated risks of misuse. They have a right to be given an informed opportunity to take steps to protect their identity. Moreover, given the speed with which identity thieves can operate, they have a right to receive accurate and prompt notification.

Yet the fact is, many organizations facing a security breach fail to notify, or they do so in an ineffective, piecemeal or untimely manner. This has been shown time and time again, in both Canada and the United States.

Why can organizations not be counted upon to notify? There is no one explanation, but the absence of any statutory duty to do so is certainly a factor. No organization, however responsible and community minded, wants the bad publicity, or the exposure to investigation or litigation that can result from publicizing security breaches. Nor does it wish to incur the associated costs, inconvenience and business disruptions – these economic incentives for systematic and effective notification of security breaches are generally lacking.

Yet, the advantages to organizations of being proactive with respect to data privacy and security, of which notification is one component, are very real. As noted by the Ontario Information and Privacy Commissioner in a 2005 presentation, these include improved customer trust, goodwill and loyalty, reduced costs associated with crisis management and damage control, and differentiation from the "rest of the pack".[19]

CIPPIC agrees with the argument referenced in the PIPEDA Review Discussion Document that having a duty to notify would force organizations to take security measures more seriously, which in turn can help to reduce identity theft.

Regrettably, however, few examples of such statutory requirement can be found in Canada. As noted in the PIPEDA Review Discussion Document, the Ontario *Personal Health Information Protection Act* requires notification in the event of a security breach.

[19] Information and Privacy Commissioner/Ontario, Identity Theft Revisited: Security is not Enough" (September 2005) at 29.

As well, while they lack legal force, the Ontario Information and Privacy Commissioner released guidelines in 2003 for government organizations to follow for security breaches. These include notification of individuals whose privacy was breached. In British Columbia, in certain conditions the *B.C. Freedom of Information and Protection Act* requires public bodies to notify affected individuals in the event of a breach.

The fact is that the U.S. is far ahead of Canada with respect to notification. Many U.S. states have passed laws requiring consumers to be notified when their personal information is compromised. California represents an especially noteworthy example of progress in this regard. Any state public sector agency and business that owns or holds computerized data that includes personal information must notify California residents, within an expedient time, of a security breach which results in acquisition of their (unencrypted) personal information by an unauthorized person.

Amending PIPEDA to require a duty to notify would fill a gap in the current Canadian legal framework. It would enable the federal Privacy Commissioner to take a leadership role in this important area, one that would hopefully be emulated by the provinces having their own privacy legislation.

Duty to Notify should be Mandatory, not Conditional

CIPPIC believes that the duty to notify should be mandatory and comprehensive. This is the only way to ensure that both the letter and the spirit of the law will be upheld by affected organizations.

Some may argue that cost and efficiency considerations and the possibility of individuals becoming "desensitized" to breach notifications mean that notification should be limited to situations where there is a serious threat of identity theft or where the information is highly personal or sensitive. However, there are problems with this reasoning.

It is not always possible to make an accurate determination of the risks associated with a security breach. Also, what is the definition of a "reasonable risk" of harm? Who would make such an assessment? Organizations themselves surely cannot be counted upon to admit to the existence of risks, let alone gauge their seriousness.

Also, individuals generally want to know if their personal information is in the hands of unauthorized entities, however small the risks of abuse. Providing the results of a risk analysis could reduce the likelihood of desensitization and enable affected individuals to take whatever protective measures they consider appropriate in a given situation. Notification procedures need not be the same for all breaches; they could be tailored to the seriousness of the situation.

It is interesting to note that the Ontario Information and Privacy Commissioner advocates that notification be mandatory, "barring exceptional circumstances"[20]. While these

[20] The State of California *Civil Code* places some boundaries on the duty to disclose security breaches. Notification is required only when unencrypted personal information, consisting of an individual's first

circumstances are not identified, it is implied that there would be few situations in which notification would not be required. The Commissioner, moreover, recommends that notification include details of the extent of the breach and the specifics of the personal information at issue, as well as information about steps that have been taken to address the breach. CIPPIC supports this approach. Organizations should be encouraged to learn from breaches and to implement measures to minimize risks of future occurrences.

The Alberta Information and Privacy Commissioner also appears to support notification of security breaches. In a recent investigation of an unauthorized release of customer information, the company concerned was advised to notify and provide assistance to customers whose personal information was or could be compromised. Furthermore, relevant credit card agencies and financial institutions were to be contacted.[21]

Notification of Security Breaches needs to be Comprehensive and Timely

CIPPIC recommends that the duty to notify be expansive. Besides the affected individuals, notification of security breaches should be directed to the Privacy Commissioner and to appropriate law enforcement and government agencies. Where it is considered that the personal information compromised could be used to commit financial fraud, relevant credit card and financial agencies should also be notified.

Notification should be immediate, to enable individuals to take steps to protect themselves against identity theft and to enable government and corporate entities to undertake mitigation measures.

The measures used should reflect the nature and seriousness of the breach. Telephone calls, e-mails, faxes, newspaper notices and the like could be used. Organizations that benefit from the collection and use of personal information should bear the costs of these notification measures and should develop policies and procedures to ensure that such measures are effective and comprehensive.

If there should be a duty to report, what sort of enforcement mechanism, if any, should be introduced to ensure that organizations comply with reporting mechanisms?

CIPPIC contends that organizations should not be themselves entrusted with self-regulation of the duty to report process. The Privacy Commissioner should have this responsibility and should be provided with adequate resources to carry out this responsibility. If a risk assessment approach is adopted, then the Office of the Privacy Commissioner should assume responsibility for risk analysis.

---

name or first initial and last name, plus one or more of a Social Security number, Driver's License number or California Identification Card number or account number, credit or debit card number in combination with any required security code, access code or password, are released.

[21] Alberta Information and Privacy Commissioner, Investigation P2006-IR-003, *Monarch Beauty Supply, a Division of Beauty Systems Group (Canada) Inc., (Re),* April 19, 2006.

If the Privacy Commissioner assumes the role of enforcement, then the ombudsman role of this Office would not be sufficient to ensure compliance. The weaknesses inherent in this approach have been discussed earlier in this submission. CIPPIC recommends that the Commissioner should act as a regulator, with the clear mandate and the necessary powers to ensure that organizations adhere to the requirement to report security breaches. These powers should include the ability to impose significant financial penalties for non-compliance.

This is not to suggest that consultation and cooperation should not be front and centre to the Commissioner's role. However, for any notification requirement to be truly effective, and for it to be perceived as such by Canadians, the Privacy Commissioner needs to have the power and resources to order compliance where it is not occurring willingly.

5. Transborder Flows of Personal Information

Does the current accountability principle in PIPEDA sufficiently protect personal information when it crosses borders?

No. Principle 4.1.3 merely requires that organizations "use contractual or other means to provide a comparable level of protection while the information is being processed by a third party". "Comparable level of protection" has been interpreted by the Privacy Commissioner as allowing disclosures to foreign governments.[22] Indeed, subss.7(3)(c.1) and (d) allow organizations to disclose without consent to "a government institution", without limiting the term "government" to Canadian government institutions. It is at least arguable, therefore, that organizations are permitted under PIPEDA to disclose customer data to other governments for law enforcement or other purposes.

This clause and its interpretation by Canadian authorities is critical in respect of Canada's trading relationship with the European Union. The EU directive, unlike PIPEDA, addresses the issue of transborder data transfers directly, prohibiting the transfer of EU personal data to countries without adequate data protection regimes.[23] Recent EU court decisions have confirmed that transfers of airline passenger data from European airlines to the US government breach EU data protection laws, because of the lack of adequate data protection in the US. One of the reasons for PIPEDA was to satisfy the European requirement for adequate data protection laws. If PIPEDA allows organizations to transfer personal data to the US, we are risking our "adequate data protection" status with the EU.

If not, how might PIPEDA better protect that information?

First, as explained above, PIPEDA should be amended to explicitly protect individuals from excessive disclosure and other inappropriate practices, including disclosures to

[22] PIPEDA Finding #313.
[23] Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data, Article 25.

foreign governments. In particular, all exceptions to the general rule of consent should be subject to a reasonableness requirement.

Second, subsections 7(3)(c.1) and (d) should be amended to make it clear that they apply to *Canadian* government institutions, not to foreign government institutions. If this amendment were made, then all foreign government requests for data about Canadians would have to go through Canadian government entities. This would be an appropriate and potentially effective safeguard against abusive foreign government practices.

Third, PIPEDA could be amended to include an explicit prohibition on disclosures to foreign governments, with significant penalties for non-compliance. Such a "blocking" provision would only be effective to the extent that its penalties were as significant to organizations as the penalties from non-compliance with foreign government orders, and only to the extent that it could actually be enforced.

Fourth, PIPEDA could be amended to include an EU-type provision prohibiting disclosures to foreign countries with inadequate data protection regimes. Countries whose data protection regimes have been found adequate (e.g,. by the Governor in Council) could be listed in a regulation. Outsourcing of data processing, as well as other disclosures, to organizations in or governments of other countries would thus be prohibited by PIPEDA. This approach would provide strong protections but would have a significant adverse effect on trade. It would need to be phased in over time in order to be fair to businesses that currently outsource data processing to the US or overseas.

Finally, the Privacy Commissioner could establish, under Principle 4.1.3, specific requirements to be included in contracts for outsourcing, such as those proposed in the Discussion paper.

5. Sharing information with other Data Protection authorities

Should PIPEDA be amended to explicitly permit the Privacy Commissioner to share information and cooperate in investigations with counterparts in other countries and with provincial counterparts in provinces that do not have "substantially similar" legislation?

Yes, PIPEDA should be amended to explicitly permit the OPC to share information and cooperate in investigations with counterparts in other jurisdictions that do not have "substantially similar" data protection legislation. Such a power would enhance the Commissioner's ability to enforce and oversee the law.

6. Other Issues:

6.1 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.

Unable to turn to the statute for guidance, and in the absence of Commissioner findings on this issue, CIPPIC's experience suggests that firms are turning to one another for instruction on acceptable dealings with children's privacy. This mode of practice appears to result in a "race to the bottom" rather than competition to provide improved privacy protection to children. Privacy policies are often written in "legalese" rather than in language tailored to minors; where firms employ child-friendly "pledges" that purport to summarize the terms of the privacy policy, the terms of the pledge and the policy often conflict.

These problems are compounded by a third: 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?

CIPPIC's view is that Canada should be paying greater attention to the privacy rights and interests of minors. The apparent dearth of complaints about children's privacy does not a lack of problems in this regard. Canada should approach the issue proactively, as other jurisdictions have, with guidelines or legislation that protect minors while offering marketers with direction in their treatment of minors. This approach should not blindly follow other jurisdictions' lead, but should be based upon social science evidence that speaks to the judgment of minors, their need for protection, and the realities of teen and pre-teen social behaviour.

6.2 Allowing opt-out of secondary uses of published telephone book data

There is a strange and inexplicable gap in the regulations specifying publicly available data: the exception for telephone directory information includes no provision allowing subscribers to opt-out of having their published information shared with other directory publishers or third parties. The only qualification of this "telephone directory exception" is that the subscriber must be entitled to refuse to have the personal information appear in the directory in the first place.

Thus, even though telephone companies are perfectly capable of giving their subscribers a choice regarding the sharing of their published data with third parties, they are not required to do so. This result is incompatible with the overall thrust of PIPEDA. The

right of telephone subscribers to opt out of secondary uses and disclosures of their contact information by the telephone company should not depend on whether or not they choose to have their information published in the directory. Those who choose to be listed in the directory do not necessarily want – and should be forced to accept – unfettered use and sharing of their data by telephone companies. All subscribers should retain that right, regardless of whether they subscribe to listed or unlisted service.

We reiterate our appreciation for the opportunity to have input into the OPC's development of its submission to Parliament during the review of PIPEDA, and hope that these comments are helpful in that respect. We would be happy to meet with the OPC at any time to discuss any of these issues at more length.

Yours truly,

original signed

Philippa Lawson
Executive Director and General Counsel
CIPPIC