PIPEDA Review Discussion Document

Protecting Privacy in an Intrusive World

July 2006

1. Purpose

The *Personal Information Protection and Electronic Documents Act* (*PIPEDA*) includes provision for a mandatory review by Parliament every five years. A review is scheduled for 2006. This discussion paper describes several issues that the Office of the Privacy Commissioner of Canada (OPC) has identified as warranting consideration in the upcoming review. This paper is not intended to set out a definitive list of issues for the *PIPEDA* review, nor does it purport to describe all the solutions for these issues. We invite those interested in privacy to comment on the issues and to raise any others that they think should be considered in the *PIPEDA* review. We welcome such input, since it will help inform the OPC as it develops its submission to Parliament during the review of *PIPEDA*.

It is not the role of this Office to draft proposed amendments to *PIPEDA*. Rather, our goal is to help Parliament and the Canadian public ensure that *PIPEDA* is the most effective vehicle possible for fulfilling Parliament's stated objective in *PIPEDA* – recognizing the right of privacy of individuals with respect to their personal information and the need of organizations to collect, use or disclose personal information "for purposes that a reasonable person would consider appropriate in the circumstances."

PIPEDA is intended to be a general and technology-neutral data protection law. This paper presents a "broad-brush" examination of *PIPEDA*, rather than a review of specific issues such as SPAM, identity theft or identity fraud. Parliament may of course decide to address these specific issues in other legislation.

2. Introduction

Several surveys over the past two decades have revealed the disquiet of Canadians about government and private sector intrusions into their privacy. Privacy, one of the hallmarks of a democratic society, is being challenged from many quarters, aided by increasingly intrusive and affordable technologies. Compounding these challenges in some cases is an attitude that privacy must be sacrificed for other social goods – national security and business efficiency prominent among them. Data mining, workplace and public surveillance, SPAM and biometric techniques such as facial recognition and DNA identification are collectively mounting a persistent attack on privacy. The same technologies that facilitate modern commerce can also facilitate identity theft and Internet fraud such as "phishing." Technologies that are harnessed for malevolent reasons can cause profound damage to the individuals whose personal information is misused.

Parliament responded to many of these privacy concerns as they related to commercial activities by enacting *PIPEDA*. *PIPEDA* was also the vehicle for Canada to provide a level of protection for personal information that would facilitate the flow of personal information from EU member states to Canada. The EU Data Protection Directive, adopted in 1995, introduced a requirement that member states allow transfers of personal information to a third country such as Canada only if the third country ensures an adequate level of protection for that information.

PIPEDA came into force in stages, beginning January 1, 2001. At that time, it covered personal information about customers that was collected, used or disclosed in the course of commercial activities by federal works, undertakings an businesses – organizations such as banks, airlines, and

telecommunications companies. The personal information of employees of such federal works, undertakings and businesses was also covered. The Act was extended to cover personal health information for these organizations and activities in 2002. *PIPEDA* was fully implemented by January 2004. As of 2004, under the Trade and Commerce power in section 91 of the Constitution, the Act was extended to cover organizations engaged in commercial activities, including those that for other purposes (for example, employment) are regulated by the provinces. *PIPEDA* therefore covers the retail sector, publishing and insurance companies, the service industry, manufacturers and other organizations, such as those in the health sector.

PIPEDA also gives individuals the right to obtain access and request correction of the personal information these organizations may have collected about them. Oversight of the Act rests with the Privacy Commissioner of Canada, who is authorized to receive and investigate complaints.

PIPEDA was not, and does not pretend to be, the answer to all the privacy issues raised by the interactions of individuals with organizations engaged in commercial activities. It provides protection only with respect to commercial activity, and even then there are several instances where it does not apply. For example, *PIPEDA* does not apply to personal information about employees of organizations that are not federal works, undertakings or businesses.

PIPEDA is relatively young legislation, and many of its provisions and the powers attached to it – audit and litigation, for example – have not been fully explored. The public has not yet taken advantage of many of the protections afforded under *PIPEDA*, and has not yet brought many of the larger privacy issues now covered by the Act the attention of the OPC. Nor has the OPC had the chance yet to "connect all the dots" between individual complaints to address the many systemic issues that we see emerging across different organizations and sectors.

That said, *PIPEDA* appears to be working reasonably well, although gaps have appeared that were not anticipated when it was drafted several years ago. Some of *PIPEDA*'s provisions may need to be reconsidered in light of experience, including the experience we have observed with substantially similar provincial privacy legislation. *PIPEDA*'s provisions may not be as effective at protecting privacy as its drafters had hoped. As well, several procedural changes and minor "housekeeping" improvements may be required to smooth the operation of the Act. Besides challenges within the legislation itself, changes in society necessitate rethinking some aspects of *PIPEDA*. These changes have occurred on many fronts – for example, the expansion in transborder flows of personal information, spyware, illegal data trafficking, increased threats to the security of computer systems and the growing interest of government agencies in personal information held by the private sector.

3. Issues to Consider

Commissioner's Powers

In designing *PIPEDA*, Parliament used an ombudsman model similar to that used for the *Privacy Act* and the *Access to Information Act.* Under all three laws, the commissioner responsible has the authority to investigate complaints, make findings and issue non-binding recommendations.

Under *PIPEDA*, the Commissioner has a limited discretion to initiate a complaint, conduct an audit and publicly disclose information relating to the personal information management practices of an organization. The Commissioner has no power to order an organization to cease or change a practice or release personal information. Nor can the Commissioner award damages. However, if an individual is not satisfied with the Commissioner's attempt to resolve certain issues, the individual has a right of review by the Federal Court. The Commissioner herself can initiate court action with the consent of the individual, and has done so on occasion where organizations have refused to implement her recommendations.

Some observers may argue that the ombudsman approach, with its lack of order-making powers, makes *PIPEDA* less effective in protecting the rights of individuals than if the Commissioner had powers of enforcement – for example, the power to order an organization to comply with a particular provision of *PIPEDA*. They may want *PIPEDA* to contain order-making powers similar to those in the British Columbia and Alberta data protection legislation. They might also look to the order-making

powers granted to the Commission d'accès à l'information du Québec under that province's *Act respecting the protection of personal information in the private sector*, the first private sector data protection legislation in Canada.

Others may suggest that the ombudsman model is preferable. They may see this model as being more accessible, informal, practical and flexible in helping parties resolve the issues between them. Supporters of the ombudsman model may also argue that *PIPEDA* does provide for binding orders through the Federal Court as the next level of enforcement, beyond the Commissioner's recommendations. Supporters of this approach might also suggest that changing the nature of the Commissioner's powers would be a complex exercise that would affect other roles of the Office – mediation, education and audit, for example – and require a reconsideration of the role of the Federal Court under *PIPEDA*.

Question

1. 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?

Consent

PIPEDA is a "consent-based" statute. Generally, it requires knowledge and consent of the individual affected for the collection, use and disclosure of personal information in the course of commercial activity. Data protection bodies around the world have struggled with the challenges of operating a consent-based regime for the processing of personal information, particularly given the modern realities of global commerce.

Reconciling the consent principle with the realities and demands of the commercial environment presents several challenges. The following discussion examines specific areas of concern relating to consent: employer/employee relationships; collection of personal information and disclosure to law enforcement and national security agencies; disclosure to investigative bodies; attempted collection, use and disclosure; individual, family and public interest exceptions to consent requirements; and blanket consent.

a. Employer/employee Relationships

PIPEDA protects the personal information of employees in a federal work, undertaking or business. Employers need personal information about their employees for many legitimate business purposes. In a perfect world with no economic coercion, the employer could ask the employee for personal information, and the employee would freely decide whether to give that information. However, given the unequal bargaining power in employment relationships, many employees may not feel in a position to withhold their consent, for fear that doing so may harm their employment or even lead to their dismissal. In such circumstances, some may argue, employees are not freely consenting to an employer's collection of their personal information, and to infer consent only because they continue to work constitutes a forced and inappropriate stretching of the consent principle that risks "watering down" the principle.

Alberta and B.C., in their *Personal Information Protection Act* (PIPA), have taken a different approach than *PIPEDA* to personal employee information. Alberta's PIPA allows an organization to collect "personal employee information" without the consent of the employee (or potential employee) under certain conditions, including when the collection is "reasonable for the purposes for which the information is being collected…." Personal employee information in Alberta's PIPA simply means personal information reasonably required by an organization that is collected, used or disclosed solely for the purposes of establishing, managing or terminating an employment relationship or a volunteer work relationship. B.C.'s PIPA allows the collection of "employee personal information" when, among other circumstances, the collection is "reasonable for the purposes of establishing, managing or terminating and employment relationship...."

Some might argue that the Alberta and B.C. provisions present a more feasible solution for dealing with the specifics of handling personal information in the modern employment context. Critics may counter that such provisions would remove from employees the autonomy to decide for themselves what is a reasonable use of their personal information and instead place the authority to make this decision entirely in the hands of their employers. Even if employees could challenge their employer's purpose by bringing a complaint, some might see this shift of power as an erosion of one's most basic and fundamental privacy right – the right to decide for oneself what is done with one's personal information.

Quebec's *An Act Respecting the Protection of Personal Information in the Private Sector* does not treat personal information about employees as a distinct category of personal information subject to special provisions. However, the test for collection of personal information about employees without their consent is based on necessity. This involves a consideration of the sensitivity of the personal information and the proportionality test articulated by the Supreme Court of Canada in the Oakes decision.[1]

Another option would be to add a specific provision to section 7 of *PIPEDA* to deal with consent issues relating to employees. As a general rule, personal information about an employee could be collection only with their consent. However, the provision could set out specific exceptions to the consent rule.

Questions:

1. 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?

2. 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?

3. Should the collection of some types of employee data be prohibited altogether? If so, what would be the criteria for prohibiting collection?

b. Collection and Disclosure for Law Enforcement and National Security Purposes

The *Public Safety Act, 2002* amended *PIPEDA* with a provision (section (7(1)(e)) that adds to the number of situations under *PIPEDA* where an organization can collect personal information without the knowledge or consent of the individual. Parliament enacted this amendment to authorize air carriers and travel agencies to collect personal information for government-run airline passenger screening systems. The amendment means that collection is permitted without knowledge or consent for the purpose of making a disclosure:

- that is required by law;

- to a government institution that has made a request for the information, identified its lawful authority to obtain the information and indicated that it suspects that the information relates to national security, the defense of Canada or the conduct of international affairs; or

- on the initiative of the organization to an investigative body, a government institution or a part of a government institution and the organization suspects that the information relates to national security, the defense of Canada or the conduct of international affairs.

Some may express concern about the broad wording of section 7(1)(e). Any organization subject to *PIPEDA*, not merely air carriers and travel agencies, now has the authority to collect personal information without knowledge or consent in the situations described in section 7(1)(e). The section does not limit the amount of information that can be collected, the duration of the collection activity or the possible sources of the information. In short, some may argue, the authority granted by the section 7(1)(e) amendment allows organizations to act as agents of the state – also described as "deputizing the private sector" – by collecting information, without consent, for the sole purpose of disclosing it to government and law enforcement agencies.

For example, this amendment to *PIPEDA* creates the potential for an organization subject to *PIPEDA* to collect personal information merely because it suspects that the information relates to the conduct of international affairs. The organization need have no legitimate business purpose for the collection of the information. The concerns about section 7(1)(e) may be heightened because the federal *Privacy Act* offers inadequate protection to personal information once government institutions obtain the information from organizations that have collected it under section 7(1)(e).

Others may argue in contrast that this amendment to *PIPEDA* is a necessary addition to the tools to address serious law enforcement and national security issues. They may argue that these are legitimate circumstances where personal information should be collected and disclosed without consent.

Questions

1. 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?

2. 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?

c. Investigative Bodies

PIPEDA permits organizations to disclose personal information, without the knowledge or consent of the individual, to an investigative body. To do so, there must be reasonable grounds to believe that the information relates to a breach of an agreement or a contravention of the laws of Canada, a province or a foreign jurisdiction. *PIPEDA* also permits investigative bodies to disclose personal information without the individual's knowledge or consent if the disclosure is reasonable for purposes related to investigating a breach of an agreement or a contravention of the laws of Canada or a province.

The authority for this comes from sections 7(3)(d) and 7(3)(h.2). Section 7(3)(d) would allow an organization to disclose information to an investigative body if the investigative body was investigating a suspected fraud or contravention of a law – for example, the defrauding of a financial institution. Section 7(3)(h.2) allows disclosure by an investigative body without consent if the disclosure is reasonable for purposes related to investigating a breach of an agreement or a contravention of the laws of Canada or a province.

The Act does not define "investigative body." Each application for the status of investigative body is confirmed by regulation. Two investigative bodies were listed when the Act came into force: the Insurance Crime Prevention Bureau and Bank Crime Prevention and Investigation Office. There are now about 75 investigative bodies. More than 20 Ontario health professional regulatory bodies such as the College of Nurses and the College of Optometrists, and the Law Societies of most provinces and territories, have been designated investigative bodies. These designations occurred on the grounds that the bodies may need to obtain personal information without consent to conduct disciplinary proceedings. Some may argue that the whole application process is cumbersome and that, given the greatly expanding number of designated investigative bodies, it is no longer clear whether this regulatory approach is the most effective. Furthermore, they may argue, bodies such as those regulating health care professionals may already offer adequate oversight of the activities of these investigative bodies.

Supporters of the current designation system may argue that the current scheme for designating investigative bodies, while cumbersome, provides much greater transparency and oversight than would a scheme that, for example, simply defined "investigative body" in *PIPEDA* and essentially allowed organizations to designate themselves as such unless the designation were successfully challenged. As well, they may argue, Privacy Impact Assessments submitted as part of the application process allow for a more open, transparent and robust approach for designation, even if the process

may be lengthy. It also allows for a clear public listing of the organizations designated as investigative bodies.

One reform option might be to attempt to define "investigative body" in *PIPEDA*. Only bodies satisfying the definition would warrant the limited special status given to such bodies. By defining "investigative bodies" in *PIPEDA*, the requirement to confirm the status of the body through regulation could be repealed, since there would be a more direct means within *PIPEDA* to determine whether a body meets the criteria for an investigative body.

Another option might be to adopt the model in the *Personal Information Protection Act* (PIPA) of both British Columbia and Alberta. The Acts both define the term "investigation" and then allow collection, use and disclosure without consent for the purposes of an investigation. For example, the B.C. PIPA defines "investigation" as an investigation related to:

(a) a breach of an agreement,

(b) a contravention of an enactment of Canada or a province,

(c) a circumstance or conduct that may result in a remedy or relief being available under an enactment, under the common law or in equity,

(d) the prevention of fraud, or

(e) trading in a security as defined in section 1 of the Securities Act if the investigation is conducted by or on behalf of an organization recognized by the British Columbia Securities Commission to be appropriate for carrying out investigations of trading in securities,

if it is reasonable to believe that the breach, contravention, circumstance, conduct, fraud or improper trading practice in question may occur or may have occurred.

The B.C. PIPA allows collection without consent if "it is reasonable to expect that the collection with the consent of the individual would compromise the availability or the accuracy of the personal information and the collection is reasonable for an investigation or a proceeding."

Questions

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

2. 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?

d. Attempted Collection without Consent

PIPEDA applies to the actual collection, use and disclosure of personal information. However, there appears to be a gap in the law relating to attempts to collect personal information without consent. For example, a 2006 decision of the Federal Court of Appeal[2] concluded that *PIPEDA* does not expressly prohibit *attempts* to collect personal information. *PIPEDA* does not apply, for example, to an attempt to collect information through video or audio surveillance with equipment that failed to work, or to an unsuccessful attempt by a bank employee to obtain information from a customer that the bank had no authority in law to acquire. Based on this reasoning, *PIPEDA* would not likely apply either to attempts to use or disclose information, when such attempts fail.

Even if, for example, an attempt to collect personal information fails, perhaps the type of collection of personal information that the organization was attempting – through secret surveillance or deceptive practices that – should entail consequences under privacy legislation for the organization making the attempt.

There is a precedent in Canadian privacy law for dealing with attempted collection. Section 59(1) of Alberta's *Personal Information Protection Act* (PIPA) generally makes it an offence to willfully attempt to gain or gain access to personal information in contravention of the Act.

Some may argue that including attempted collection in *PIPEDA* could give the complainant a right to have the Federal Court hear the complaint, make a binding order and even award damages. Section 16 permits the Court to grant a range of remedies, including an order to the organization to correct its practices and publish a notice of any action taken or proposed to be taken to correct its practices. The Court may also award damages to the complainant, including damages for any humiliation that the complainant has suffered.

Questions:

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

e. Individual, Family and Public Interest Exceptions to Consent Requirements

This consent principle finds expression in clause 4.3 of the Schedule to *PIPEDA*. Clause 4.3 states, in part, that the "knowledge and consent of the individual are required for the collection, use, or disclosure of personal information, except where inappropriate." Section 7 of *PIPEDA* acknowledges the consent principle in clause 4.3, but identifies several specific situations where information may be collected, used or disclosed without the knowledge or consent of the individual. For example, section 7(3)(e) allows a disclosure without an individual's knowledge or consent "to a person who needs the information because of an emergency that threatens the life, health or security of an individual and, if the individual whom the information is about is alive, the organization informs that individual in writing without delay of the disclosure."

Some situations are not covered by this or any other provision, such as disclosures to the family of an injured, ill or deceased individual, or disclosures in the public interest after a major disaster.

Question

1. 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?

f. Blanket Consent

As noted elsewhere in this discussion paper, *PIPEDA* is a consent-based statute. It generally requires consent for the collection, use and disclosure of personal information in the course of commercial activity. The prevailing view might be that as long as a consent clause is worded broadly enough, this will technically and legally permit a wide range of future collections, uses and disclosures under the terms of the agreement between the customer and the organization. However, others may argue 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. They may see consent as giving them the opportunity to receive further explanations and to ask questions or challenge assumptions – particularly in relationships of unequal bargaining power.

On the other hand, others may argue that consumers are generally free to determine the extent of the consent they are giving to the collection, use and disclosure of their personal information, and that no changes to *PIPEDA* are needed to make consent more meaningful. They may also argue that many consumers don't want to be asked for their consent to every specific type of collection, use and

disclosure of their personal information, and that they may become annoyed if too frequently asked to make a choice or fill out another form.

Question

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

Disclosure of Personal Information before Transfer of Businesses

PIPEDA contains no provision to allow an organization to disclose personal information to prospective purchasers or business partners without the consent of the individual affected. They may need to review this information (such as client lists) for their "due diligence" evaluation of whether to proceed with the transaction – perhaps a merger, acquisition or sale of business. Such transactions may range from the relatively modest – the sale of a dental practice, including its patient lists – to very large corporate takeovers.

Other laws, such as Ontario's *Personal Health Information Protection Act* (PHIPA) and the Alberta and British Columbia *Personal Information Protection Act* (PIPA) allow disclosures without the individual's consent, subject to stringent confidentiality agreements. Some may argue that it is appropriate to include a similar provision in *PIPEDA*. They may conclude that this would both facilitate commercial transactions and protect commercial secrets in a highly competitive environment.

If a sale or merger occurs, some individuals may not want their personal information transferred as part of that sale or merger. Some may argue that individuals should have the opportunity to opt out of the transfer of their personal information where possible. In some cases, however, regulatory requirements oblige retaining personal information for a period of time. Individuals whose personal information is at stake could be made aware of this through proper notification up front.

Questions:

1. 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?

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

Work Product

PIPEDA does not use or define the term "work product." B.C.'s *Personal Information Protection Act* (PIPA), on the other hand, defines work product in part as "information prepared or collected by an individual or group of individuals as a part of the individual's or group's responsibilities or activities related to the individual's or group's employment ..." Some may argue that a definition of work product such as that in B.C.'s PIPA would bring greater certainty to the concept of work product and facilitate rules in *PIPEDA* for applying distinct rules to work product.

Such a definition might also make more clear the distinction between "work product," "business information," and "contact information," and thus allow for differentiating how they are to be treated under *PIPEDA*.

If work product is defined, *PIPEDA* can treat it in one of three ways:

- Exclude work product from the definition of "personal information" in *PIPEDA*. *PIPEDA* would then not apply to such information at all. An example of this approach is found in B.C.'sPIPA, as described above;

- Consider work product to be personal information (that is, include work product in the definition of personal information), but state that the data protection provisions of *PIPEDA* do not apply to the information. This is the approach *PIPEDA* takes, for example, with personal information collected, used or disclosed for journalistic, artistic or literary purposes;

- Include work product in the definition of personal information, but state that the consent requirements found in section 7 of *PIPEDA* do not apply to work product. Other provisions of *PIPEDA* would continue to apply to work product. For example, section 3, the "purpose" section, would continue to apply even if the consent provisions did not. Collection, use or disclosure of work product information would still therefore be subject to the test in section 3 that balances the right of privacy of individuals with the need of organizations for that information.

Some may argue that excluding work product from the definition of "personal information" or stating that the data protection provisions of *PIPEDA* do not apply (the first two approaches described above) may mean that *PIPEDA* cannot be used to provide oversight of and challenge some forms of surveillance. For example, surveillance of workers through video, audio, or keystroke surveillance of their workplace activities might not fall under *PIPEDA* if the records of the surveillance are considered to be work product.

Quebec's *An Act Respecting the Protection of Personal Information in the Private Sector* provides an example of how work product information – in this case personal information on professionals about their professional activities – can be made the subject of provisions tailored to the nature of the information. In 2001, a provision was added to the Act giving an enhanced discretion to grant access to personal information on professionals about their professional activities. In this way, some may argue, the Quebec Act treats work product information as being situated mid-way between personal and non-personal information. The Commission d'accès à l'information may, on written request, grant a person authorization to receive communication of personal information on professionals regarding their professional activities, without the consent of the professionals concerned. This access is subject to the following criteria:

- previous consultation with the professional Order concerned;

- respect for professional secrecy;

- the professional will be notified periodically of the intended uses and ends contemplated;

- the professional will have an opportunity to opt-out;

- security measures are in place to ensure confidentiality of information.

The authorizations must be revised annually, and the list of authorized persons is published.

Questions:

1. Should *PIPEDA* define "work product"?

2. If so, how should *PIPEDA* treat work product?

Duty to Notify

Identity theft can occur electronically on a massive scale if organizations fail to provide adequate security to personal information they have collected. Some may argue that organizations that suffer security breaches ("involuntary disclosures") or the outright theft of their personal information holdings should be required to mitigate the risk of identity theft to the individuals involved. Mitigation after a security breach could involve notifying the individuals whose information is at stake, credit agencies,

relevant government agencies (for example, those that administer benefits such as welfare) and other commercial entities, such as banks.

By the end of 2005, roughly half of U.S. states had passed laws requiring customers to be notified when their personal information is compromised. As well, several bills have been introduced, but none yet passed, at the federal level in that country. These laws typically provide for large fines for failure to notify. For example, legislation in New York State provides for penalties of up to $150,000 for knowingly or recklessly violating the reporting requirements.

Of Canadian data protection laws, Ontario's *Personal Health Information Protection Act* is the only one requiring notification after a security breach. The Act requires health information custodians to notify individuals at the first reasonable opportunity if their personal health information is stolen, lost, or accessed by unauthorized persons.

Some may argue that *PIPEDA* should include a similar duty to notify the individuals affected after a security breach. As well, section 7(3) of *PIPEDA*, dealing with disclosures without consent, could be amended to permit an organization that has suffered a security breach to notify credit bureaus and other relevant organizations or agencies about the breach. Once alerted, credit bureaus could place fraud alerts on the files of the affected individuals. In addition, *PIPEDA* could be amended to require notifying the Privacy Commissioner of a breach.

Some may argue that laws requiring organizations to notify individuals of security breaches will force those organizations to take security more seriously, to avoid their security failings becoming public knowledge. This in turn may help reduce identity theft and other fraudulent uses of personal information. On the other hand, critics of "notice" laws may argue that it is expensive for organizations to carry out notifications. They may also argue that consumers will start to ignore the notices, particularly if notices are required after any breach, not merely if the breach creates a risk of fraud. If notice laws were to be enacted, those critics might want the laws to require an assessment of risk or severity of the potential harm; this would avoid trivializing the effect of notifications over time by diluting the more important notices amidst a flood of others that may not be necessary or even appropriate. For example, reporting might be required only if the loss or theft creates a reasonable likelihood that the personal information will be used to the detriment of the individual affected, or if the loss affects large numbers of records. In addition, some may argue that conditions should be articulated to guide the implementation of notices in different circumstances to avoid causing potentially more unnecessary harm to the individuals concerned. They may also argue that for notification laws to be truly effective, organizations must take steps after the notification to minimize the risk of further security breaches.

Questions:

1. 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?

2. 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 requirements?

Transborder Flows of Personal Information

The current business climate often favours the outsourcing of data processing. Some outsourcing results in the transfer of personal information to organizations in Canada that are themselves subject to *PIPEDA* or substantially similar provincial data protection legislation. Outsourcing may also involve transferring personal information outside Canada, a process described as the transborder flow of personal information.

In the current climate of globalized business and increasingly inquisitive of foreign governments, protecting personal information as it flows across borders has assumed even greater urgency.

PIPEDA contains an accountability principle that imposes responsibility on an organization for information that has been transferred to a third party for processing. Clause 4.1.3 of the Schedule to

PIPEDA requires the organization to use contractual or other means to provide a comparable level of protection while the information is being processed by a third party. This principle applies to any transfer, whether the receiving company is in Canada or abroad.

The concern about loss of control over personal information of Canadians when it crosses borders has led to discussion about several possible options to enhance respect for this accountability principle. Among the other means to protect personal information are provisions that might be placed in contracts between an organization in Canada subject to *PIPEDA* and the receiving company, such as provisions:

- allowing the organization to inspect and audit the information management practices of the receiving company processing the data abroad, including security practices and disposal procedures, and how the receiving company will enforce these practices and procedures;
- requiring the receiving company to provide individuals with access to the personal information it holds about them;
- prohibiting use and disclosure by the receiving company, except as required by the law of the country in which the receiving company is situated;
- ensuring that the enforcement of the contract takes place in a suitable jurisdiction;
- calling for binding arbitration in accordance with international rules of arbitration.

Questions:

1. Does the current accountability principle in *PIPEDA* sufficiently protect personal information when it crosses borders?
2. If not, how might *PIPEDA* better protect that information?

Sharing Information with Other Data Protection Authorities

In general, *PIPEDA* requires the Commissioner to treat as confidential any information that is obtained in the exercise of the Commissioner's powers. The Commissioner may publicize the information practices of an organization if the Commissioner considers it in the public interest to do so. As well, the Commissioner may disclose information in the course of a prosecution of certain offences or a hearing or appeal before the Federal Court.

Section 23 of *PIPEDA* permits the Commissioner to consult with any person whose powers and duties under substantially similar provincial legislation are like those of the Commissioner. The Commissioner can enter agreements with counterparts in provinces with substantially similar legislation to coordinate the activities of their respective offices for handling any complaint in which they are mutually interested. In practice, this means, for example, that the Commissioner can share information and cooperate in investigations of mutual interest with counterparts in Ontario (only with respect to Ontario health information custodians), Alberta, British Columbia and Quebec. However, there is no specific authority for the Commissioner to share information and cooperate in investigations with other provinces.

In addition, complaints do not always fit neatly within Canada's national borders. Some may argue that the growing importance of transborder data flows – for processing purposes, to facilitate e-commerce, for law enforcement and national security purposes, or simply as a result of people going about their daily lives – highlights the need for information sharing and cooperation in investigations with organizations outside Canada. While *PIPEDA* allows the Commissioner to share information and cooperate in investigations with certain provincial counterparts, there is no specific authority to do so with other jurisdictions. Canadians might have greater comfort with transborder data flows, for example, if there were a mechanism for the Commissioner to enter arrangements with oversight

bodies in other jurisdictions to facilitate the exchange of information, which might in turn lead to more effective enforcement. The Commissioner might also be given the power to assist in investigations and audits in foreign jurisdictions.

Questions:

1. 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?

2. Are there other organizations with which the Commissioner should be able to share information and cooperate?

4. Comments

Comments on this discussion paper and other suggestions for reform of *PIPEDA* may be sent to the Office of the Privacy Commissioner of Canada by September 7, 2006:

Office of the Privacy Commissioner of Canada
PIPEDA Review
112 Kent Street
Place de Ville
Tower B, 3rd Floor
Ottawa, Ontario
K1A 1H3

Email address for comments: consultation@privcom.gc.ca

For all general inquiries, please contact:

Toll-free: 1-800-282-1376
Phone: (613) 995-8210
Fax: (613) 947-6850
TTY: (613) 992-9190

Our hours of service are from 9 a.m. to 5 p.m.

---

[1] *Laval (Ville de) v. X*, [2003] IIJCan 44085 (C.Q.), referring to *R. v. Oakes*, [1986] 1 S.C.R. 103, 1986 CanLII 46 (S.C.C.).

[2] *Morgan v. Alta Flights (Charters) Inc.*, 2006 FCA 121.