THE CANADIAN BAR ASSOCIATION
L'ASSOCIATION DU BARREAU CANADIEN
The Voice of the Legal Profession
La voix de la profession juridique

September 13, 2006

Ms. Jennifer Stoddart
Privacy Commissioner of Canada
Office of the Privacy Commissioner of Canada
112 Kent Street
Place de Ville
Tower B, 3rd Floor
Ottawa, Ontario
K1A 1H3

Dear Commissioner:

Re: PIPEDA Review Discussion Document

The Privacy and Access Law Section of the Canadian Bar Association (CBA Section) is pleased to have this opportunity to comment on the PIPEDA Review Discussion Document (Discussion Document). The CBA is a national professional organization of over 36,000 members, including lawyers, notaries, law students and teachers, with a mandate that includes improvement in the law and the administration of justice. The CBA Section consists of lawyers specializing in privacy and access to information law from every Canadian jurisdiction.

In August 2005, the CBA Section prepared a submission to Industry Canada, entitled "Preparing for the 2006 Review of the *Personal Information Protection and Electronic Documents Act*". As many of the issues addressed in the Discussion Document are those discussed in our previous submission, we have co-related previous relevant recommendations to our response to the points raised in the Discussion Document. For the sake of completeness, we have included questions from the Discussion Document to which the Section has not yet had sufficient time to develop a recommendation. The 2005 submission is attached for your reference.

(i) *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?

Recommendation

The CBA Section recommends that PIPEDA should follow the tribunal model adopted by the Canadian Human Rights Commission.

An impartial, rotating panel should be established with order-making powers and ability to award damages, with a cap on general damages. The Office of the Privacy Commissioner should retain investigative powers and advocacy role. If the Commissioner determines that a complaint is "well founded", the Commissioner should be required to issue a finding within six months and this finding should be referred to the tribunal. Both complainants and respondents would be able to seek judicial review of a decision of the tribunal.

(ii) ***Consent***

a. Employer/employee Relationships

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?

Recommendation

The CBA Section recommends adopting the model set out in Alberta PIPA for employers' handling of employee information, as its "reasonableness" component adequately protects against abuses, such as wholesale or unnecessary surveillance activities.

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

No Recommendation

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

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 the 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?

The CBA believes that, where there is a reasonable expectation of privacy, any disclosure of personal information to law enforcement must comply with existing constitutional standards. The CBA most recently expressed this position in the context of internet service providers' initiatives to monitor subscriber information for potential disclosure to law enforcement, and related lawful access proposals.

The focus of the Association's concerns is "the profound impact on the privacy of individual Canadians, and particularly on the potential to destroy solicitor client privilege by seizing communications between lawyers and clients." (A copy of the CBA's July 5, 2006 letter to Federal Ministers is attached).

c. Investigative Bodies

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?

Recommendation

The CBA Section recommends that:

- **section 7(3)(d) of *PIPEDA* be replaced with the following text: "made by an organization where reasonable for the purposes of an investigation or legal proceeding",**

- ***PIPEDA* be revised to adopt the approach in the B.C. and Alberta PIPAs, and Manitoba Bill 200, permitting collection, use and disclosure without consent where reasonable for the purposes of an investigation, and**

- **the definition of "investigation" set out in the Alberta PIPA be adopted, in particular the requirement that "it is reasonable to conduct an investigation".**

Recommendation

The CBA Section recommends that the investigative body provisions of PIPEDA be replaced with provisions that:

(a) adopt the approach in the B.C. and Alberta PIPAs and Manitoba Bill 200, so that any consent exception for disclosure "mirror" consent exceptions for collection and use;

(b) adopt the approach in the B.C. and Alberta PIPAs and Manitoba Bill 200, permitting collection, use and disclosure without consent where reasonable for the purposes of an investigation; and

(c) adopt the approach, found expressly in the B.C. PIPA, and arguably implicitly in Alberta PIPA and Manitoba Bill 200, that there is no additional consent required for a third party processor, such as an investigator, to collect, use and disclose personal information on behalf of an organization.

d. Attempted collection without consent

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

No Recommendation

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

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?

Recommendation

The CBA Section recommends that *PIPEDA* adopt a two-part approach as in sections 7(1) and 8 of the B.C. PIPA, so an individual provides implied consent where:

- **the purposes would be considered obvious to a reasonable person, and the individual voluntarily provides the personal information to the organization for that purpose; or**

- **the individual is provided with information as to the purposes, the individual has the opportunity to decline but does not do so, and the collection, use and disclosure is reasonable having regard to the sensitivity of the personal information in the circumstances.**[1]

The CBA Section recommends that *PIPEDA* address the issue of consent obtained indirectly from an individual through another person. An organization should be permitted to rely, acting reasonably, on an assurance or on surrounding circumstances that a person providing personal information of another individual has consent of the other individual for the specific purposes involved, or that the other individual would consent if aware of the circumstances (a donation or gift). Factors in assessing the reasonableness of this reliance include the nature of the transaction, the sensitivity of the personal information, whether the collection, use or disclosure benefits the individual, the nature of the relationship between the individual and the person confirming the individual's consent, and apparent authority given by one individual to deal with another individual, and should be explicitly listed, although the list need not be exhaustive.

f. Blanket Consent

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

No Recommendation

---

[1] See section 7 and 8(3) of the B.C. statute.

(iii) ***Disclosure of Personal Information before Transfer to Business***

1. Should *PIPEDA* allow an organization in possession of personal information to disclose that information to a perspective 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?

Recommendation

The CBA Section recommends that *PIPEDA* be amended to clarify the business transaction provisions, similar to section 22 of Alberta PIPA.

(iv) ***Work Product***

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

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

Recommendation

The CBA Section recommends that the definition of "personal information" be clarified, and explicitly exclude "business or professional information", defined as:

> **Information that enables an individual at a place of business to be contacted, including the individual's name, position or title, the business address, telephone number, fax number or e-mail address, or a professional designation or registration number identifying an individual. It also includes a description of the professional or official responsibilities of the individual, and information prepared or collected by an individual or group as part of the individual's or group's responsibilities or activities related to employment or business.**

(v) ***Duty to Notify***

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?

Recommendation

The CBA Section recommends that, if a duty to notify is to be directly or indirectly included in PIPEDA, it should adopt a balanced approach (for example, using California's SB 1386 as a model). For example, a duty to notify might include where:

1. **information is about an identifiable individual or the information is not identifiable by virtue of being protected through, for example, encryption or de-identification, the organization has received notice that such protection has been breached, and**

2. **information falls in one of certain specified categories of sensitive personal information that could be used for identity theft purposes, such as Social Insurance Numbers, sensitive financial information (including bank account numbers), and health information.**

(vi) ***Transborder Flows of Personal Information***

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?

Recommendation

The CBA Section recommends that where personal information is to be stored or processed in a jurisdiction outside Canada, *PIPEDA* require additional provisions in contracts between organizations and entities storing or processing personal information for organizations, to enhance security of the personal information and ensure conformity to Canadian law.

(vii) ***Sharing Information with Other Data Protection Authorities***

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?

No Recommendation

Thank you for the opportunity to contribute this response to your Discussion Document. We trust it will be of assistance in preparing your submission to the upcoming Parliamentary Committee review process. Please feel free to contact me should you or members of your office wish to discuss these issues further.

Yours truly,

Original signed by Gaylene Schellenberg for Brian Bowman

Brian Bowman
Chair, National Privacy and Access Law Section

Preparing for the 2006 Review of the *Personal Information Protection and Electronic Documents Act*

NATIONAL PRIVACY AND ACCESS LAW SECTION
CANADIAN BAR ASSOCIATION

August 2005

TABLE OF CONTENTS

Preparing for the 2006 Review of the *Personal Information Protection and Electronic Documents Act*

PREFACE

The Canadian Bar Association is a national association representing 34,000 jurists, including lawyers, notaries, law teachers and students across Canada. The Association's primary objectives include improvement in the law and in the administration of justice.

This submission was prepared by the National Privacy and Access Law Section with assistance from the Legislation and Law Reform Directorate at the National Office. The submission has been reviewed by the Legislation and Law Reform Committee and approved as a public statement of the National Privacy and Access Section of the Canadian Bar Association.

Preparing for the 2006 Review of the *Personal Information Protection and Electronic Documents Act*

I. EXECUTIVE SUMMARY

The Canadian Bar Association Privacy and Access Law Section (CBA Section) welcomes the opportunity to provide input to Industry Canada for the 2006 Committee Review of the *Personal Information Protection and Electronic Documents Act* (PIPEDA).[1]

Our views are guided by the CBA's August 2004 resolution entitled "Privacy Rights in Canada." The resolution (attached as Appendix A) encourages vigilance in monitoring and opposing unnecessary erosions of privacy by both government and non-governmental organizations. It supports fair information practices as set out in the CSA's Model Code (Schedule 1 to PIPEDA). More specifically, it urges that all collection, use and disclosure of personal information without consent be conducted only in a manner that is reasonable and necessary and in accordance with consent or clearly stated exceptions to the consent requirement. It encourages the harmonized development of privacy legislation and practices across Canada. Our views are also consistent with those set out in the CBA's 1999 submission on Bill C-54*, Personal Information Protection and Electronic Documents Act.*[2]

We have recommended that the government refine several of the current provisions of PIPEDA to,

---

1 SC. 2000, c. 5. Available online at: http://www.privcom.gc.ca/legislation/02_06_01_01_e.asp.

2 CBA Resolution 04-05-A; Submission on Bill C-54 (99-11), *Personal Information Protection and Electronic Documents Act* (Ottawa: CBA, 1999).

(i) clarify the internal working of the statute, and

(ii) amend the legislation by adding certain provisions to achieve more consistency between federal and provincial privacy laws.

Many provinces have, in fact, drafted legislation to address uncertainties in PIPEDA that have become apparent. We believe that the amendments we suggest will provide much needed clarity to enhance organizational compliance, as well as the public's awareness and ability to exercise its privacy rights.

One of the most commonly expressed concerns about PIPEDA is the structure of the statute, that is, the Act plus a Schedule format. A number of the principles set out in the Schedule are expressly negated or modified by the provisions of the Act. For individuals without legal training, this makes understanding and exercising their rights under the Act especially difficult. Smaller organizations that wish to comply with the Act but cannot afford legal counsel are similarly challenged.

Optimally, all requirements should be in the statute itself, making it easier to understand and assisting in the harmonization of federal law with provincial statutes. In the event that Industry Canada decides not to restructure the statute to this extent, we have recommended specific, targeted refinements consistent with the guiding criteria of our 2004 resolution.

We address both specific provisions of the Act and general issues pertinent to several sections of the Act. While our analysis results in some repetition, it highlights how the various provisions are inextricably linked, and accordingly, the importance of consistent drafting throughout the legislation. Four key issues serve as examples: the treatment of employee information, business transactions, impacts on the litigation process and law enforcement.

Our discussion of employee information addresses to whom the Act applies, that is the need to clarify the scope of employee information that is not governed by PIPEDA. We consider the appropriate consent requirements for certain activities involving employee information under PIPEDA, and recommend following British Columbia and Alberta's *Personal Information Protection Act*s' (PIPA) treatment of employee information.

Similarly, we consider "business transactions" in the context of difficulties in complying with PIPEDA's consent requirements for activities such as due diligence in mergers and acquisitions, and outsourcing of business processes, including investigations within and outside of Canada. In addition to examining how individual consent may operate in these transactions, we consider the relationship between an organization and third party processors, agents and investigative bodies. The pros and cons of several options are discussed in light of concerns about disclosure of the personal information of Canadians outside of the country.

PIPEDA should be neutral in regard to the litigation process by specifically excluding personal information collected, used or disclosed in relation to litigation. The current exceptions relating to litigation are too narrow and should, at a minimum, be broadened to ensure that well-established litigation procedures are not impeded. There should be a broad exclusion for information legally available to a party to a proceeding that would override specific exceptions currently found in PIPEDA.

Related to this concern, PIPEDA should be amended in the way it applies for law enforcement purposes, specifically in the provisions for collection, use and disclosure of personal information without consent for legitimate law enforcement

purposes.[3] The current provisions relating to investigations and enforcement of laws are overly narrow, confusing and internally inconsistent. A single standard should be applied for collection, use and disclosure relating to law enforcement, and the provisions respecting "investigative bodies" should be clarified. Organizations should be permitted to carry out their own investigative activities without unnecessarily being required to use other investigative bodies to collect information from third parties.

Clarifying key definitions such as "commercial activity", "personal information" and "identifiable", and including new definitions for "collect", "use" and "disclose", would improve all areas of the Act. With our discussion on clarifying the scope of the application of PIPEDA, we recommend clarifying both which organizations and what types of information are subject to the Act. We also discuss expanding the powers of the Commissioner's Office, as well as notification of loss and remedies for privacy breaches.

In summary, we hope that our input will help to ensure that a review of PIPEDA will achieve improvements to make it more workable and more consistent with other privacy legislation in Canada. Clarifying the legislation would benefit both Canadian citizens and organizations, and be consistent with the purposes of PIPEDA:

> …to establish… rules to govern the collection, use and disclosure of personal information in a manner that recognizes 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.

3 See also CBA Resolution, *supra*, note 2, which urged governments to "better preserve, promote and respect privacy, and specifically to ensure that the needs of government to collect, use and disclose personal information in relation to national security and law enforcement are subject to reasonable and attainable objectives and respect the privacy of individual Canadians to the maximum extent possible, having due regard to the right of individual Canadians to security of the person and to the benefit of the rule of law."

II. DEFINITIONS

A. Commercial Activity

Section 4(1) states that organizations that collect, use or disclose information "in the course of commercial activities" are subject to PIPEDA. The definition of "commercial activities" as "any particular transaction, act or conduct or any regular course of conduct that is of a commercial character, including the selling, bartering or leasing of donor, membership or other fundraising lists", is circular and vague.

This deficiency is apparent in relation to the Canadian health care sector where both the nature and the scope of "commercial activities" are unclear and open to debate. For example, it is arguable whether physicians working in private offices but paid by a public health care insurance system are pursuing a "commercial activity". Illustrating this ambiguity, seventy-five *Questions and Answers* were developed to assist in interpreting the statute for the health care system.[4] While that initiative was intended to reduce the inherent uncertainty, even it contains broad caveats, such as,

> ***NOTE:*** *The following answers are preliminary and very general in nature and may vary in particular circumstances depending on the specific circumstances of the situation.*

The current definition of "commercial activity" has been particularly challenging to apply both in the health and the not-for-profit sectors. The definition is clearly "transaction" based, but uncertainty arises as to what specific transactions of a non-commercial entity are to be considered a "commercial activity". The answer is complicated by the *Questions and Answers* prepared by the Alberta Commissioner on the application of the Alberta PIPA[5] to non-profit organizations, as well as corresponding information

4 Developed in 2003 by Industry Canada and others as PIPEDA Awareness Raising Tools (PARTs) Initiative for the Health Sector.

5 Available online at: http://www.psp.gov.ab.ca/index.cfm?page=faqs/NotProfitFAQs.html.

from the Federal Commissioner's office.[6] While both Commissioners have indicated that fundraising, a key objective of many non-profit organizations, is not a "commercial activity", the legislation should be clear. In addition, it should be clarified whether charging fees for activities, such as courses or for membership, constitutes a "commercial activity".

RECOMMENDATION:

The National Privacy and Access Law Section of the Canadian Bar Association recommends that the definition of "commercial activity" be clarified to enumerate activities of non-commercial entities that are of a "commercial character", including selling, bartering or leasing donor, membership or other fundraising lists, but excluding activities such as fundraising.

B. Personal Information

The definition of "personal information" should be clarified to be consistent with both the Federal Commissioner's finding in PIPEDA Case Summary #15,[7] and the exclusion of "work product information" in the B.C. PIPA, which in effect codifies the Commissioner's finding. Certainty as to the scope of PIPEDA is critical for business organizations to ensure that all information simply referring to an employee is not considered the personal information of that individual for the purposes of access. In addition, codification of this exclusion would recognize, as did the Federal Commissioner and the B.C. Act, that just because information "relates" to an individual, it is not necessarily "about" them in a personal sense.

6 Available online at: http://www.privcom.gc.ca/fs-fi/02_05_d_19_e.asp.

7 Available online at: http://www.privcom/gc.ca/media/an/wn_011002_e.asp.

This exclusion may be contrasted with the Assistant Commissioner's finding in PIPEDA Case Summary #303[8] that the number of houses sold by real estate agents in a year was their personal information. Not only is such information clearly "about" these individuals, it represents financial information about those agents' income. However, the finding in that case did not expressly distinguish the finding in Case Summary #15. This has generated some uncertainty about the "work product" exception set out in case Summary #15, an exception that has governed organizations' treatment of business records since the early days of PIPEDA's enactment. Amending PIPEDA to codify the "work product" distinction in Case Summary #15 would resolve this uncertainty, and also conform to the expressed policy intent of Industry Canada when the legislation was developed.

In addition, only the "name, title or business address or telephone number of an employee of an organization" are currently excluded from the definition of personal information. This category should be expanded to recognize business realities and the manner in which organizations communicate with clients. It should be consistent with Alberta and B.C. PIPAs, which exclude business e-mail and fax numbers from the definition of personal information, although in Alberta, business contact information may only be used to contact the individual in their professional or business capacity. Finally, the exclusion for business contact information should apply to people like independent contractors and consultants, not only to "employees".

Another situation that has generated confusion is that where one individual expresses an opinion about a second individual. Is the opinion then the personal information of the first individual, the second individual, or both? This is of particular significance in the case of records for employees of federal works, undertakings and businesses.

8 Available online at: http://www.privocm.gc.ca/cf-dc/2005/303_20050531_e.asp.

RECOMMENDATION:

The National Privacy and Access Law Section of the Canadian Bar Association recommends that the definition of "personal information" be clarified, and explicitly exclude "business or professional information", defined as:

> **Information that enables an individual at a place of business to be contacted, including the individual's name, position or title, the business address, telephone number, fax number or e-mail address, or a professional designation or registration number identifying an individual. It also includes a description of the professional or official responsibilities of the individual, and information prepared or collected by an individual or group as part of the individual's or group's responsibilities or activities related to employment or business.**

The Act is also inconsistent with respect to exclusions from the definition of "personal information". These elements, such as name, title or business address or telephone number of an employee of an organization, may well also appear in a professional directory as described in paragraph 1(b) in the *Regulations Specifying Publicly Available Information*, in which case they are considered to be "personal information". Accordingly, if all such data elements are clearly excluded from the definition of "personal information", paragraph 1(b) should be reexamined.

C. Collect/Use/Disclose

Organizations may deal with personal information without an individual's consent depending on whether the activity is a "collection", "use" or "disclosure". In our view, definitions for these terms are required. This is particularly important where an organization "transfers" personal information to a third party for processing or otherwise engages a third party to perform a service dealing with the organization's personal information, where an organization receives unsolicited personal information, and where personal information is stolen from an organization.

RECOMMENDATION:

The National Privacy and Access Law Section of the Canadian Bar Association recommends that PIPEDA should include the following definitions:

"Collect" in relation to personal information means to gather, acquire, receive or obtain the information by an organization or on its behalf by any means, including, subject to the provision below, on an unintended or unsolicited basis, from any source external to the organization. "Collection" has the corresponding meaning.

Collection does not include "use". It is also not a collection if personal information was received by the organization on an unintended or unsolicited basis and the organization immediately returns the personal information to the sender without using or retaining a copy.

"Use" in relation to personal information in the custody or under the control of an organization or a person means to handle or deal with the information, including by a third party on behalf of and at the direction of the organization, but does not include disclosure of the information. "Use" as a noun has a corresponding meaning.

"Disclose" in relation to personal information in the custody or under the control of an organization means to intentionally[9] make the information available or to release it to the custody or control of another organization or to another person.

D. Identifiable

Under PIPEDA, information is not "personal" if it is not about an "identifiable" individual. As such, this distinction is critical to the application of the Act. Organizations require legislative guidance on when information is and is not about an identifiable individual.

9 We suggest the qualifier "intentionally" in the definition of "disclose" to exclude unintentional disclosure such as theft, where clearly the "disclosure" was unauthorized. However, we recognize this may have implications for the term as more generally used under Principle 7 - Safeguards. If such an inclusion would have the unintended consequence of limiting application of the Safeguards principle, alternatives should be considered.

RECOMMENDATION:

The National Privacy and Access Law Section of the Canadian Bar Association recommends that the Act should include a new definition of "identifiable" that requires two elements before information may be said to be about an "identifiable" individual in the hands of the organization:

- **the organization must have the legal and technical capacity to use the data to identify an individual. For example, in cases:**

  (a) where the organization holds both the identifiers and the information within the same entity,

  (b) where the organization holds the identifiers and the information in separate entities with an agreement between the entities regarding the use of the personal information, or

  (c) where the separate entities are affiliates, having the ability to cause the other entity to provide the organization with the information and/or identifiers, as applicable) when there is no legal/contractual prohibition about "re-engineering" the information and the organization has the technical capability to do so; and

- **where only reasonable efforts are required to make the individual identifiable – the requirement for extreme or unusual effort would exclude the information from the definition of "identifiable".**

E. Government Institution

The term "government institution" is not defined, though it is incorporated by reference in section 7(3)(c.2) to "the government institution mentioned in section 7 of the *Proceeds of Crime (Money Laundering) Act*." No such reference is provided with respect to what entities may constitute a "government institution" for the purposes of section 7(3)(c.1). Given that such disclosures may be made by an organization without the knowledge or consent of the individual, organizations should be aware of what entities constitute "government institutions" to ensure that they are not inadvertently breaching an individual's privacy by making such a disclosure.

RECOMMENDATION:

The National Privacy and Access Law Section of the Canadian Bar Association recommends that the Act include a definition of "government institution" to clarify whether disclosure is intended to encompass disclosure to municipal, provincial, territorial, federal and non-Canadian entities.

III. APPLICATION

Section 4 deals with the scope and application of PIPEDA, and its relationship with other statutes. It is critical to providing reasonable certainty about whether individuals and organizations, and/or their activities, are subject to PIPEDA. As currently drafted, section 4 lacks the requisite certainty in at least three respects: definitions, exclusions and primacy. We have previously addressed definitional issues. Exclusions and primacy are addressed below.

A. Clarifying the Scope of Employee Information Excluded from PIPEDA

PIPEDA does not apply to personal information about employees who are not employees of federal works, undertakings or businesses (non-FWUB employees). However, PIPEDA does apply to personal information of non-FWUB employees to the extent not related to their employment. Some practitioners are using the Alberta or B.C. PIPA definition, for example, "collected, used or disclosed solely for the purposes reasonably required to establish, manage or terminate an employment relationship", for guidance as to what information about a non-FWUB employee is "employee personal information" and so, not governed by PIPEDA. However, a more explicit description of the scope of information about non-FWUB employees not governed by PIPEDA would be helpful.

RECOMMENDATION:

The National Privacy and Access Law Section of the Canadian Bar Association recommends that that a definition or

clarification be added to more clearly delineate the line between personal information that is not employee personal information of employees of non-federal works and their employee personal information.

B. Specific Exclusions

Several specific exclusions from the application of PIPEDA should be added to the three exclusions now found in section 4(2). These include court documents (see B.C. PIPA, section 3(2)(e) and Alberta PIPA, section 4) and other related exclusions as set out in provincial personal information protection acts. We recognize that a wholly unregulated approach to court records (currently exempted under section 2(d) of the *Publicly Available Information Regulations*) should be very carefully considered, and only in the broader context of expanding the availability of court records, for example, over the Internet.

RECOMMENDATION:

The National Privacy and Access Law Section of the Canadian Bar Association recommends that consideration be given to expanding the enumerated exclusions in section 4(2) to align more closely with the approach of the B.C. and Alberta PIPAs.

C. Transfers between Provincial Privacy Law Jurisdictions

PIPEDA's application to inter-provincial disclosure and transfers of information between two or more provinces that have personal information protection acts that have been found to be substantially similar to PIPEDA has generated significant confusion. A set of principles governing how the third piece of legislation (PIPEDA) should be practically applied would be helpful.

RECOMMENDATION:

The National Privacy and Access Law Section of the Canadian Bar Association recommends that that a set of principles be developed clarifying the application of PIPEDA to inter-provincial disclosure/transfers of information between two or more provinces where provincial personal information protection acts have been found to be substantially similar to PIPEDA.

D. Relationship to *Privacy Act*

Finally, section 4(3), addressing the relationship between PIPEDA and other statutes, should clarify the interplay between PIPEDA and the federal *Privacy Act*. In sum, PIPEDA should be more precise as to which of those two statutes has primacy. Private sector organizations providing services to federal government institutions are frequently frustrated because they cannot determine conclusively which law has priority in the context of the service relationship.

RECOMMENDATION:

The National Privacy and Access Law Section of the Canadian Bar Association recommends that section 4 of PIPEDA clarify the interplay between PIPEDA and the federal *Privacy Act* with respect to private sector organizations performing work for public sector institutions.

E. Relationship to Provincial/Territorial Access to Information Legislation

Consideration should be given to adding government institutions to which provincial/territorial public sector privacy legislation applies to section 4(2)(a). Some government institutions are covered by both those public sector privacy laws and by PIPEDA. This is true of government institutions to which Crown immunity does not apply, that is any institution governed by these laws other than government ministries. Entities that may be engaged in commercial activities in relation to personal information must determine whether there is an express

contradiction such that the federal privacy legislation would prevail over the provincial/territorial privacy and access law.

This has caused considerable confusion. We suggest that provincial and territorial government institutions be excluded from PIPEDA in the same way as their federal counterparts. Furthermore, as with the federal *Privacy Act*, the application of PIPEDA to private sector organizations that perform work for provincial/territorial public sector institutions should be clarified.

RECOMMENDATION:

The National Privacy and Access Law Section of the Canadian Bar Association recommends that section 4 of PIPEDA be extended to exclude provincial/territorial public sector institutions covered by provincial/territorial privacy and access law in the same manner as it does with respect to the federal *Privacy Act.*

IV. SPECIFIC EXCEPTIONS TO THE REQUIREMENT FOR CONSENT

A. Collection for Statistical Study or Research Purposes

Problems have arisen in the exception in sections 7(2)(c) and 7(3)(f) related to collection for statistical study or research purposes. There is no similar exception for collection, and the requirements to inform the Commission before the information is used are sufficiently burdensome that many organizations do not comply. Even if all organizations acted in strict compliance, the Commissioner's office would be unable to handle all such inquiries.

Section 2(1) of the B.C. PIPA provides a more comprehensive procedure for dealing with statistical or research purposes. The procedure places specific conditions on an organization before disclosing or using such information, and relieves both organizations and the Commissioner's office from dealing with these issues every time such a project is undertaken.

In addition, the word "impracticable", meaning impossible, clearly seems not to be the meaning intended by sections 7(2)(c) and 7(3)(f). In our view, this is far too high a standard to be met.

RECOMMENDATIONS:

The National Privacy and Access Law Section of the Canadian Bar Association recommends that the B.C. PIPA procedure be adopted, with refinement to provide greater clarity on the "security and confidentiality conditions", similar to Schedule 1 of PIPEDA. The exception in sections 7(2)(c) and 7(3)(f) should be available at the time of collection.

We also recommend that the word "impracticable" be changed to "impractical".

B. Reciprocal Collection/Disclosure Rules

One of the main criticisms of section 7(1), (2), (3) exceptions in PIPEDA for collection, use and disclosure, is their lack of symmetry. For example, although an organization may disclose personal information without knowledge or consent for the purposes of debt collection, there is no parallel authority to collect or use the information for the same purpose. Similarly, an organization may disclose information to its legal counsel under section 7(3)(a), but apparently has no comparable exception allowing it to collect or use the information in the same manner unless another exception applies. The absence of parallel exceptions,

such as those in the specific exceptions to collection, use and disclosure in both B.C. PIPA and Alberta PIPA, creates practical difficulties for organizations.

RECOMMENDATION:

The National Privacy and Access Law Section of the Canadian Bar Association recommends that changes to PIPEDA similar to those creating parallel exceptions in B.C. PIPA and Alberta PIPA be considered, and a "safety value" for symmetrical application be created to further avoid any confusion, such as that in section 18(3) of B.C. PIPA.

C. Required or Authorized By Law

The section 7(3)(i) exception is limited to *mandatory* legal requirements, and fails to include permissive legislative provisions. B.C. PIPA and Alberta PIPA have added "authorized by law" to address the lacuna in PIPEDA. A similar provision is contained in section 6 of Quebec's Act regulating the *Protection of Personal Information in the Private Sector* (Quebec Act), permitting collection from third parties without consent if authorized by law.[10] There is also confusion as to whether provincial/territorial, foreign or the common law is included in the applicable law. Consideration should be given to clarifying the exception's application to foreign laws (for example, when a treaty allows for intentional cooperation between Canada and another country, as in the case of money laundering.)

RECOMMENDATION:

The National Privacy and Access Law Section of the Canadian Bar Association recommends that section 7(3)(i) should include matters "authorized by law" as provided in provincial legislation, and should clarify which law applies.

10 *Act Respecting the Protection of Personal Information in the Private Sector*, 1993, section 6.

D. Breach of Laws

Again, this is an issue of symmetry and consistency. For example, breach of a foreign law is not in the exception to collection in section 7(1)(b). It is referenced in the related investigative section, except in sections 7(2) and (3) for use and disclosure.

RECOMMENDATION:

The National Privacy and Access Law Section of the Canadian Bar Association recommends increased consistency in applying exceptions for breaches of the laws of Canada, a province or territory, or a foreign jurisdiction with each of the related section 7 exceptions.

E. Litigation

The exceptions relating to litigation under PIPEDA are too narrow and if strictly applied, could unintentionally impede well-established forms of litigation practices (similar issues are raised in connection with rights of access in the litigation process). Our principal concerns are:

- the narrowness of the investigation exception (section 7(1)(b))(see related discussion, *infra*),
- the one-way disclosure to a barrister or solicitor (section 7(3)(a)),
- the collection and use of debt disclosure information (section 7(3)(b)), and
- the limitation of disclosures in the litigation process, inadequately covering all aspects of the process - pleadings, oral discovery, mediation, private arbitration, settlements, solicitor communications and other non-court ordered exchanges of information (see section 7(3)(c)).

RECOMMENDATION:

The National Privacy and Access Law Section of the Canadian Bar Association recommends adopting the models for litigation provided in B.C. and Alberta PIPAs, including a broad exclusion for information available by law to a party in a proceeding.

F. Business Transactions, Due Diligence

There has been considerable confusion in the business community over the meaning of due diligence in the course of business transactions. PIPEDA generally requires consent before disclosing personal information in the ordinary course of many business transactions. However, on a strict interpretation, PIPEDA appears to only apply to asset sales, and not share transactions.

Requiring consent is frequently inappropriate in business transactions as it can contravene securities laws, deter buyers and/or interfere with confidentiality obligations. It is often impractical to obtain consent from individuals (including individual employees) for disclosure of personal information deemed necessary for due diligence and completion of business transactions. It can be a cumbersome or nearly impossible administrative task, significantly impeding the business transaction. Disclosing the transaction destroys the confidentiality often necessary for business or competitive reasons. Further, individuals may withhold consent for ulterior motives, for example, employees desiring to enhance severance demands.

The business transaction provisions in Alberta and B.C. PIPAs ensure that parties enter into an agreement to protect the privacy of personal information that is exchanged. They also require that the use of such information is restricted where necessary for the parties to determine whether to proceed with the business transaction, and if so, for the parties to carry on and complete the transaction. In our view, business transactions should be conducted in the normal course. At present, organizations often assume that implied consent applies (for example, that customers, employees and tenants "know" a business must be sold) without being entirely sure if PIPEDA supports this assumption. The business community requires clear rules. A better model is found in section 22 of Alberta PIPA.[11]

11 See commentary at p.p. AB-97-102 in Platt, Hendlisz, Intrator and Kaufman, *Privacy Law in the Private Sector, An Annotation of the Legislation in Canada*, Canada Law Book, Release No. 3, Dec 2004.

RECOMMENDATION:

The National Privacy and Access Law Section of the Canadian Bar Association recommends that PIPEDA be amended to clarify the business transaction provisions, similar to section 22 of Alberta PIPA.

G. Employee Information

PIPEDA applies to personal information of employees of federally regulated employers. Under the current legislation, federally regulated employers must obtain employee consent for the collection, use and disclosure of employee personal information. However, such consent can be less than voluntary if employees fear direct or indirect repercussions if they refuse consent. Also, it can be administratively quite cumbersome to obtain individual consent from a large number of employees for such matters as hiring employees and administering the employment relationship.

Adequate protection of employee personal information can be achieved where:

- the employer is obliged to collect, use and disclose personal information for reasonable purposes for recruitment and administering the employment relationship,
- the collection, use and disclosure of employee personal information is subject to a privacy policy that is administered by the employer's privacy officer,
- employees are informed of the purposes for the collection, use and disclosure of employee personal information,
- employees have access to review their personal information to ensure it is accurate and compel corrections, and
- the employer is under an obligation to reasonably safeguard the confidentiality of employee personal information.

To effectively administer the employment relationship, employers require exceptions to the general privacy principles to investigate breaches of employment policy, work rules, the law and terms and conditions of employment. In many circumstances, to require employee consent prior to the investigation

would defeat the integrity of the investigation, for example, in a workplace harassment investigation or audit. A "reasonableness" test would facilitate such investigations.

Finally, employers should be able to exchange personal employee information with benefits providers for the purpose of administering employment benefits, without needing specific employee consent.

RECOMMENDATION:

The National Privacy and Access Law Section of the Canadian Bar Association recommends adopting the model set out in Alberta PIPA for employers' handling of employee information, as its "reasonableness" component adequately protects against abuses, such as wholesale or unnecessary surveillance activities.

H. Journalistic Exception

Certainly, there must be an exception for most forms of journalism, as freedom of expression is constitutionally protected in Canada. However, the right to privacy is also a fundamental Canadian value. A balance between these important, and often colliding interests is required.[12]

RECOMMENDATION:

The National Privacy and Access Law Section of the Canadian Bar Association recommends that the journalistic exception be defined more clearly to find an appropriate balance between freedom of expression and privacy. As well, the relationship

12 This balance has recently been considered by the House of Lords in *Campbell* (Appellant) v. *MGN Limited* (Respondents) [2004] UKHL 22, where the privacy rights of model Naomi Campbell prevailed over the tabloid press. This issue also surfaced over the full disclosure of personal information of Tsunami victims over the objections of their families.

between the specific exceptions and the blanket exemption for organizations (section 4(2)(c)) should be clarified.

I. Literary Exception

Similar to the exceptions for journalism, the scope of "literary" purposes should be clarified. For example, it is unclear whether the "literary" exception would include correspondence such as a legal memorandum or opinion.

RECOMMENDATION:

The National Privacy and Access Law Section of the Canadian Bar Association recommends that the scope of "literary" purposes be clarified.

V. THIRD PARTY PROCESSORS, AGENTS, AND INVESTIGATIVE BODIES

A. Third Party Processor

Under Principle 4.1.3, PIPEDA appears to treat information transferred to a third party for "processing" as being in the possession or custody of the client organization, such that the third party is effectively considered part of the organization. PIPEDA also requires that the client organization use contractual or other means to ensure a comparable level of protection while the information is being processed by a third party.

Since such processed information is not in the custody of the third party processor but rather in the custody of the client, any transfer between the client and the third party processor has generally not been interpreted as disclosure. Accordingly, consent has not been required.

Two positions have developed on the issue of whether "processing" includes "collection" by a processor or only "transfers" between client and the processor.

B. Processing includes Collection

A number of sources support the position that processing includes collection.

1) Agency concept generally

While in many cases service providers may not be acting as legal agents in the strict sense, the service provider is acting on behalf of the organization such that the common law principle of agency - that is, that an agent may do what its principal may do - should apply. It is illogical that, for example, disclosures by an organization of contestant addresses to a mailing, or promotions fulfillment house would not require consent, but collection by a fulfillment house, rather than by the organization directly, would require specific consent identifying the fulfillment house. As long as,

(i) the fulfillment house is collecting only on behalf of the organization and is restricted from using the personal information for any other purpose, and

(ii) the organization itself is collecting such information in accordance with PIPEDA,

it is difficult to see how omitting the applicable consent of a specific reference to the fulfillment house would prejudice an individual whose personal information is collected.

2) Comments of former Privacy Commissioner

During a speech in March 2003,[13] the former Privacy Commissioner discussed the scope of the third party processor exception, and, in summary stated that there was no need to designate private investigators as "investigative bodies" given that investigators act as agents for their clients. He also noted that an investigator retained by an individual client for personal or domestic purpose (for example, to

13 Speech made by the former Privacy Commissioner to the Private Investigators Association of British Columbia.

determine if a spouse is hiding assets) would not be considered retained in connection with a commercial activity, and the individual client would not be governed by PIPEDA. The investigator, as an agent of the individual, is also not governed by PIPEDA.

3) *Ferenzcy* v. *MCI Medical Clinics* (Ontario Superior Court)[14]

The first consideration by a court of the relationship between an investigator and a client for the purposes of PIPEDA occurred in *Ferenzcy*. The court made two points, in *obiter*. As it was actually the defendant collecting the information for personal use, consent was not required. The activity was not a commercial activity and, more significantly, "those whom the [i.e. the defendant] employs are merely his agents". In effect, the investigator, as a third party processor collecting information on behalf of the client, was able to do without consent what his client was able to do without consent.

4) B.C. PIPA, and *Ontario Personal Health Information Protection Act* (PHIPA)

One of the most persuasive arguments supporting the position that the scope of the third party processing exemption should include collection activities is the need for national harmonization. For example, the B.C. PIPA includes a concept of "agent", in the case of collection, as:

> An organization may collect personal information from or on behalf of another organization without consent of the individual to whom the information relates, if
>
> (a) the individual previously consented to the collection of the personal information by the other organization, and
> (b) the personal information is disclosed to or collected by the organization solely
>
> (i) for the purposes for which the information was previously collected, and
> (ii) to assist that organization to carry out work on behalf of the other organization.

While Alberta PIPA does not contain a similar provision, or any provision with respect to third party processing, the common law principle that an agent may do what its principal may is likely to apply. The draft of Manitoba's Private

14 (2004) 70 O.R. (3d) 277.

Member's Bill 200, the *Personal Information Protection Act* similarly omitted such a provision, but the same rationale regarding the agency principle would seem to apply.

C. Processing does not include Collection

Organizations are currently faced with reconciling the points canvassed above with Industry Canada's contrary comments in the *Regulatory Impact Analysis Statement* for the original *Regulations Specifying Investigative Bodies*. It states that without the exception in PIPEDA that permits an investigative body to disclose information back to the organization for which it is conducting an investigation,

> the flow of information could only go in one direction, from the organization to the investigative body. The investigative body would be unable to disclose the results of its investigation back to its client or other interested parties without consent.

In addition, officials in the Office of the Privacy Commissioner have suggested that the processor exception should be strictly limited to transfers of personal information by an organization to a third party for processing (for example, payroll processing, pensions and benefits administration). Such comments indicate that the remarks made by the former Commissioner in his March 2003 speech may have been too broad.

RECOMMENDATION:

The National Privacy and Access Law Section of the Canadian Bar Association recommends that PIPEDA be amended to confirm the existence of an "agent" concept, through an amendment to clarify the third party processing rule in Principle 4.1.3, to confirm that an organization may collect, use and disclose personal information from or on behalf of a principal organization without the consent of the individual to whom the information relates, if (a) the individual previously

> **consented to the collection, use and disclosure of the personal information by such principal organization, and (b) the personal information is collected, use and disclosed by such organization to assist that organization to carry out work on behalf of the principal organization.**

D. Investigative Bodies

1. Collection Consent Exceptions for Investigations

The exemption in section 7(1)(b) permits an organization to collect personal information without consent if it is reasonable to expect that requiring knowledge and consent would compromise the availability or accuracy of the information, and the collection is reasonable for purposes relating to investigating a breach of an agreement, laws of Canada or laws of a province or territory.

We question whether such collection should be limited only to where obtaining consent would "compromise the availability or accuracy of the information". At times, obtaining consent will not compromise the availability or accuracy of information, but will actually jeopardize the investigation. For example, the subject of the investigation may leave the jurisdiction.

Industry Canada might, in practice, interpret the requirement quite broadly. In the *Regulatory Impact Analysis Statement* for the *Regulations Amending the Regulations Specifying Investigative Bodies*, it states:

> Organizations with investigative body status would be able to disclose personal information in their investigations without the consent of the individual only in those exceptional circumstances in which obtaining consent is impossible, impractical or *undesirable because it would frustrate the conduct of the investigation*. (emphasis added)[15]

15 Canada *Gazette*, Part I (November 8, 2003) at 3529.

The disclosure consent exemption in section 18(1)(c) of B. C. PIPA also more broadly states that "it is reasonable to expect that the disclosure with the consent of the individual would compromise an investigation or proceeding…".

RECOMMENDATION:

The National Privacy and Access Law Section of the Canadian Bar Association recommends that section 7(1)(b) of PIPEDA be modified to say: "would compromise the investigation, and the collection is reasonable…".

2. Disclosure Consent Exception for Investigations (Disclosure to Investigative Body)

The exemption in section 7(3)(d) permits an organization to disclose personal information to an investigative body on its own initiative if the organization has reasonable grounds to believe that the information relates to a breach of agreement or of laws of Canada, a province, or a foreign jurisdiction that has been, is being, or will be committed.

If an investigative body requests the information from a third party organization, will the disclosure by the third party be considered of its "own initiative"? More significantly, if the organization is itself permitted to collect information under section 7(1)(b) in connection with an investigation, there should be a separate disclosure consent exemption so the organization will not have to retain an investigator to effectively collect from third parties? Without such an exemption, third parties are technically unable to disclose to an organization collecting under section 7(1)(b) without consent. Do the disclosure requirements under section 7(3)(d) effectively render the consent exemption for collection under section 7(1)(b) meaningless where collecting from third parties?

It seems logically inconsistent to permit an organization to collect without consent for an investigation, but then to effectively prevent it from collecting from third parties in connection with that investigation without first hiring an investigative body.

In contrast, Alberta PIPA and Manitoba Bill 200 permit collection and use without consent where disclosure is permitted without consent. They also allow for the disclosure of personal information without consent where reasonable for the purposes of an investigation or legal proceeding. The B.C. PIPA similarly permits collection and use without consent where disclosure is permitted without consent. It allows for disclosure without consent where it is reasonable to expect that the disclosure with the consent of the individual would compromise an investigation or proceeding, and the disclosure is reasonable for purposes related to an investigation or a proceeding.

RECOMMENDATION:

The National Privacy and Access Law Section of the Canadian Bar Association recommends that:

- **section 7(3)(d) of PIPEDA be replaced with the following text: "made by an organization where reasonable for the purposes of an investigation or legal proceeding",**
- **PIPEDA be revised to adopt the approach in the B.C. and Alberta PIPAs, and Manitoba Bill 200, permitting collection, use and disclosure without consent where reasonable for the purposes of an investigation, and**
- **the definition of "investigation" set out in the Alberta PIPA be adopted, in particular the requirement that "it is reasonable to conduct an investigation".**

3. Disclosure Consent Exception for Investigations (Disclosure by Investigative Body)

Section 7(3)(h.2) of PIPEDA permits an investigative body to disclose personal information without consent (for example, to its client) where the disclosure is reasonable for purposes related to investigating a breach of agreement or of the laws of Canadian or a province.

As the result of these somewhat intricate investigative body consent exemptions, numerous bodies have applied for, and some have successfully obtained, investigative body status. Unfortunately, a number of the organizations that have applied are professional regulatory organizations (for example, medical colleges or provincial branches of the Certified General Accountants Association). Such organizations do not appear to be involved in investigations in connection with commercial activities such that PIPEDA would even apply, yet their applications were accepted.

If a private investigator is effectively an agent of an organization, and so a third party processor pursuant to the broader interpretation of the term as set out above in our discussion of third party processors, we question the need for these complicated investigative body provisions permitting disclosure between an investigator and its client. It is also unclear why organizations that do not appear to be governed by PIPEDA in any case have been granted investigative body status under the regulations.

PIPEDA's "investigative body" consent exceptions are problematic in that they:

(a) lead to confusion regarding the application of principles of agency law;

(b) have unnecessary qualifications; for example, requiring that:

   i. all organizations must disclose on their "own initiative"

   ii. collection without consent in connection with an investigation only occur where obtaining such consent would compromise the availability or accuracy of the information

(c) are inconsistent with, and thus detract from, harmonization with the approach taken in a number of provincial privacy regimes

(d) lead to inconsistent results, in that an organization may have the right to collect without consent in connection with an investigation, but effectively cannot do so from third parties as such parties do not have the right to disclose without consent, and

(e) have inadvertently led to confusion regarding the scope of the application of PIPEDA. Organizations that *prima facie* do not appear to be involved in commercial activities and would seem not to be governed by PIPEDA have voluntarily submitted applications to be investigative bodies to Industry Canada, and those applications have then been accepted. This leads to the interesting question of whether PIPEDA would apply if such an organization were to breach its pre-conditions to be investigative body, given that PIPEDA otherwise does not appear to apply to these non-commercial activities.

RECOMMENDATIONS:

The National Privacy and Access Law Section of the Canadian Bar Association recommends that the investigative body provisions of PIPEDA be replaced with provisions that:

(a) adopt the approach in the B.C. and Alberta PIPAs and Manitoba Bill 200, so that any consent exception for disclosure "mirror" consent exceptions for collection and use;

(b) adopt the approach in the B.C. and Alberta PIPAs and Manitoba Bill 200, permitting collection, use and disclosure without consent where reasonable for the purposes of an investigation; and

(c) adopt the approach, found expressly in the B. C. PIPA, and arguably implicitly in Alberta PIPA and Manitoba Bill 200, that there is no additional consent required for a third party processor, such as an investigator, to collect, use and disclose personal information on behalf of an organization.

VI. ACCESS REQUESTS

In our view, the exemptions from the right of access should be simplified and made more workable. We have a number of suggestions that we believe would further those objectives.

A. Applicable to all Exemptions

Section 9 would be more simple and practical if all the exemptions were listed in one section. We note that the emphasis of PIPEDA is on access to "information", not on "records" *per se*. The references in PIPEDA to severance are therefore somewhat confusing, though they are generally perceived as having been added for greater certainty. It would be more accurate for the provision to state:

> If the information about the individual includes information about the third party, the third party information should be severed from the information about the individual before giving the access to the individual.

An ability to "refuse to confirm or deny" the existence of information that may be exempt should also be added. This should apply to all exemptions, to ensure that its use does not denote the type of information at issue.

It should also be stated that there is no right of access under this Act where a right of access or a duty of confidentiality exists under another statute or regulation or rule made under an Act. In particular, it should be clear that the right of access does not interfere with the rules applicable to litigation either before a court or tribunal. Where there is a duty of confidentiality or implied undertaking under the rules for discovery, this Act cannot provide a right of access. As well, as with solicitors' liens, where another Act prevents a client from obtaining his or her file from his or her lawyer's office until payment has been made, PIPEDA cannot authorize access to the file where payment is outstanding.

B. Investigations of Breaches of a Law or Agreement

This exemption is difficult to understand and so would be difficult to implement. The current wording allows organizations to respond beyond 30 days and to notify the Commissioner. In our view, as it is the only exemption that allows this to happen without notice, it fails to protect the confidentiality of the investigation. Anyone making such a request would be alerted that a law enforcement matter or other investigation is taking place or had taken place.

The duty to notify the Commissioner is also overly cumbersome. Additional steps appear unnecessary, as individuals can complain when the exemption is claimed, as with any other exemption, and the Commissioner may then decide if necessary. The Commissioner may notify affected parties, such as police authorities, to determine the efficacy of the claim for the exemption.

RECOMMENDATION:

The National Privacy and Access Law Section of the Canadian Bar Association recommends that the exemption for investigation of breach of a law or agreement should be clarified to allow it to apply to any information which, if disclosed, could interfere with an internal or external investigation, or a law enforcement matter, in respect of a breach of a law or agreement or the right of an individual to a fair trial. The right to conduct internal audits or reviews should also be authorized absent consent, so that the refusal to confirm or deny provision would allow organizations to claim the exemption without compromising an investigation.

C. Formal Dispute Resolution

RECOMMENDATION:

The National Privacy and Access Law Section of the Canadian Bar Association recommends that all efforts at mediation or settlement of a matter remain confidential, and that this exemption provision be extended broadly to all such matters.

D. Confidential Commercial Information

This exemption is neither clear nor sufficiently broad. There is ambiguity as to whether "employee promotion information" is "commercial". For example, an organization assessing which are its most valuable staff members could find that access to information requests before a decision is released do not fall within the exemption. Similarly, where the organization is determining who should receive an award, or succeed in a job competition, confidential information about applicants will be involved. In our view, there should be a discretionary exemption.

RECOMMENDATION:

The National Privacy and Access Law Section of the Canadian Bar Association recommends that this exemption for confidential commercial information should be clarified and broadened.

E. Threatening the Life or Security of Another Individual

On occasion, disclosure of information, such as medical information, could prejudice the mental or physical health of the requester as well as "another" individual.

RECOMMENDATION:

The National Privacy and Access Law Section of the Canadian Bar Association recommends that he exemption involving threats to the life or security of another individual should be broadened to include the requester personally.

F. Substitute Decision Makers

Specific reference should be made to the right of certain persons acting in the place of an individual to obtain access to the individual's information, such as custodial parents of children under a stipulated age, persons with powers of attorney, personal representatives of individuals, or persons who ought to receive information in the place of others on a compassionate basis (such as where a deceased dies intestate and the close family members wish information).

RECOMMENDATION:

The National Privacy and Access Law Section of the Canadian Bar Association recommends that specific reference be made to the right of certain persons acting in the place of an individual to obtain access to the individual's information.

G. Settlement Privilege

Settlement privilege is recognized at common law, but it does not appear to be part of solicitor-client privilege.

RECOMMENDATION:

The National Privacy and Access Law Section of the Canadian Bar Association recommends that PIPEDA should recognize settlement documents as an exemption from the right of access.

VII. ENFORCEMENT POWERS

A. Expansion of Powers, Remedies

The main remedy employed by the Commissioner's office under PIPEDA has been to post a summary of formal findings made as a result of a section 11 complaint on their website. The formal findings will conclude that the complaint is "well founded", "not well-founded" or "resolved", and provides the complainant with a right to apply to the Federal Court for specified relief.

In January 2004, the Commissioner's office began to settle complaints during the course of an investigation or implementing early resolutions before commencing an investigation. These are also posted on the Commission's website. As such, the Commissioner is cast in the role of an ombudsperson and does not have an effective compliance power.

This can be seen as a one-sided approach that does not provide the organization with similar recourse for erroneous findings or unfounded complaints. Also, the two-step procedure to obtain a remedy in Federal Court can be criticised as overly time-consuming and costly. Federal Court remedies are limited. Notably, no damage awards have been made since the enactment of PIPEDA. Complainants and their counsel may well fear that the cost of proceeding will outweigh any benefit gained from such an award.

In addition, many complaints are inappropriate and unnecessarily burdensome on organizations. The Commissioner's 2004 Annual Report states that 41% of the complaints were determined to be not well-founded.

There are no rules or process guidelines for investigations conducted by the Commissioner's office. Investigations take a considerable period of time (sometimes up to 9 months), and insufficiently protect solicitor-client privilege.

At times they turn into fishing expeditions by delving into matters beyond the subject of the particular complaint.

Many involved with PIPIDA have commented that the ombudsperson model established for the Privacy Commissioner is ineffective and results in significantly reduced compliance. Companies that handle personal information simply do not fear the consequences of being found to be acting contrary to PIPEDA. The Commissioner may only issue "findings", none of which bind any of the parties involved. The Commissioner's office has begun to follow-up and to ask respondents to report on changes they have made, but neither the follow up nor a response is mandatory.

The lack of order-making powers significantly affects complainants. To obtain a remedy or compensation, complainants must apply to the Federal Court, but they may only a do so once the Commissioner has issued a finding. At present, it takes as long as a year to receive a finding. Also, taking a matter to the court effectively requires hiring legal counsel, and places the complainant at risk of an award of costs. Further, there is no mechanism for the Commissioner to provide compensation to an individual who has incurred significant expense or suffered loss in connection with the complaint.

Conferring order-making powers on the Commissioner as the role is currently structured may result in a violation of principles of fundamental justice. The Commissioner is meant to advocate in favour of personal information protection in both the private and the public sectors. The Commissioner's office also investigates alleged violations of PIPEDA. Having an "advocate" and investigator also sit as a decision-maker may place the Commissioner in a conflict of interest and undermine the credibility of the office.

RECOMMENDATION:

The National Privacy and Access Law Section of the Canadian Bar Association recommends that PIPEDA should follow the tribunal model adopted by the Canadian Human Rights Commission.

An impartial, rotating panel should be established with order-making powers and ability to award damages, with a cap on general damages. The Office of the Privacy Commissioner should retain investigative powers and advocacy role. If the Commissioner determines that a complaint is "well founded", the Commissioner should be required to issue a finding within six months and this finding should be referred to the tribunal. Both complainants and respondents would be able to seek judicial review of a decision of the tribunal.

It is important to note that our recommendation for order-making powers is conditional on adopting an impartial tribunal model.

Businesses have expressed concern that even with honest efforts to comply, they are left with considerable uncertainty about what is required under PIPEDA. There is a definite issue as to whether, and, to what extent, the Federal Court will defer to findings of the Privacy Commissioner.[16]

To remedy these problems, the Commissioner should be authorized to issue "advance rulings" or to provide advance guidance to organizations requesting it. Such powers could emulate Canada Revenue Agency's guidance to taxpayers, as long as the assumptions or factual basis upon which advice is based remains

16 Compare this to Alberta's PIPA, sections 36(3), 52.

unchanged. This suggestion could only be meaningfully implemented however if a tribunal were established and the Commissioner was precluded from "prosecuting" an organization for following prior guidance.

The advance ruling function of the Office of the Privacy Commissioner could also be implemented on a cost-recovery basis.

RECOMMENDATION:

The National Privacy and Access Law Section of the Canadian Bar Association recommends that PIPEDA be amended so that the Commissioner is authorized to issue "advance rulings" or to provide advance guidance to organizations requesting it. Such powers could emulate Canada Revenue Agency's guidance to taxpayers, as long as the assumptions or factual basis upon which advice is based remains unchanged. For effective implementation, a tribunal should be established, and the Commissioner should be precluded from "prosecuting" an organization for following prior guidance.

As originally passed, PIPEDA does not allow an organization to ignore repeated, frivolous or vexatious access requests or complaints from individuals. PIPEDA does not provide a mechanism to deal with a large number of related requests from different individuals that may be calculated to harass the organization.

RECOMMENDATION:

The National Privacy and Access Law Section of the Canadian Bar Association recommends that PIPEDA be amended to permit organizations to ignore an individual who has shown a pattern of access requests or complaints that could reasonably be characterized to be frivolous or vexatious. To avoid fear of sanction, the organization should first report to the Commissioner the details surrounding anything it proposes to

treat as a vexatious or frivolous complaint, and the individual should have the right to complain. The Commissioner should have jurisdiction to make a finding on the issue.

For individuals, the costs associated with making an application to the Federal Court are often prohibitively expensive. The recent experience of Mathew Englander before the Federal Court – Trial Division,[17] shows that an individual complainant may be faced not only with legal fees associated with the proceeding, but with an award of costs. Likewise, an organization faced with a baseless complaint may be forced to incur significant legal fees to proceed to the Federal Court.

RECOMMENDATION:

The National Privacy and Access Law Section of the Canadian Bar Association recommends that the Office of the Privacy Commissioner or the Department of Justice should have funding to assist individual complainants in applications to the Federal Court where complaints are significant and raise substantial issues.

At present, PIPEDA provides only complainants and the Privacy Commissioner with access to the Federal Court after a finding has been issued. As a finding is not a "decision" for the purposes of the *Federal Courts Act*, there is no possibility of an organization seeking judicial review of a finding or other pronouncement of the Commissioner. This may appear reasonable as in most cases the Federal Court is the avenue for an aggrieved individual to seek a remedy. However, there are also circumstances where principles of fundamental justice suggest that an organization should be able to initiate a proceeding in the Federal Court. For example, the Privacy Commissioner may publicize information about an organization's personal information management practices without possible

17 *Englander v. Telus Communications Inc.* [2003] FCT 705.

liability. Findings and incident summaries can besmirch an organization's reputation, but may ultimately be erroneous on factual and legal grounds. Even findings that do identify a specific entity can impact not only upon a particular business, but also organizations that engage in similar practices. To ensure that the correct legal interpretation will prevail, respondent organizations should be able to appeal the finding of the Commissioner on the basis of an error of law.

Other considerations to streamline the complaints process and remedial redress available under PIPEDA are:

- require the complainant to exhaust other recourses prior to filing a complaint (Alberta PIPA, section 46(3)),
- protect privilege during the course of an investigation (Alberta PIPA, section 40),
- provide guidelines for investigations in Schedule 1,
- provide more effective damage remedies to address issues including whether damages should be limited to the actual loss, how to qualify a loss of privacy, whether an organization should profit from a deliberate mass privacy breach motivated by profit, and
- expand the whistle-blower protection to other persons in organizations with knowledge of privacy breaches.

B. Notification of Loss

To date, federal and provincial privacy legislation has required public and private organizations to adopt security safeguards when handling personal information. While similar legislation exists in the United States, recent U.S. legislative and judicial developments have imposed and/or may impose an additional legislative requirement on organizations; namely, the duty to notify individuals in the event of a security breach involving improper disclosure of their personal information. In contrast, Canadian privacy legislation does not explicitly contain such a requirement, with the exception of PHIPA.

Notification of privacy breaches is addressed in the following examples of existing or pending legislation or case law:

1. PHIPA: Section 12(2),[18]
2. California's SB 1386,[19]
3. *United States Notification of Risk to Personal Data Act,*[20]
4. C*omprehensive Identity Theft Prevention Act* (SB 768),[21] and
5. *Bell et al. v. Michigan Council 25 of the American Federation of State, County, and Municipal Employees*.[22]

RECOMMENDATION:

The National Privacy and Access Law Section of the Canadian Bar Association recommends that, if a duty of notify is to be directly or indirectly included in PIPEDA, it should adopt a balanced approach (for example, using California's SB 1386 as a model). For example, a duty to notify might be included where:

1. **information is about an identifiable individual or the information is not identifiable by virtue of being protected through for example, encryption or de-identification, the organization has received notice that such protection has been breached, and**
2. **information falls in one of certain specified categories of sensitive personal information that could be used for identity theft purposes, such as Social Insurance Numbers, sensitive financial information (including bank account numbers, credit card numbers, or personal identification numbers), and health information.**

---

18 *Personal Health Information Protection Act* (Ontario), S.O. 2004, c. 4, s. 12(2).

19 *An Act to Amend, Renumber, and Add Section 1798.82 of, and to Add Section 1798.29 to the Civil Code*, *relating to Personal Information*, California Senate Bill 1386 (2002).

20 *United States Notification to Risk to Personal Data Act*, U.S. House of Representatives Bill 1069 (109th Congress).

21 *Comprehensive Identity Theft Protection Act*, U.S. Senate Bill 768 (109th Congress).

22 *Bell et al v. Michigan Council 25 of the American Federation of State, County and Municipal Employees*, AFL-CIO Local 1023, Michigan Court of Appeal, Feb. 15, 2005.

C. Whistleblower Protection

Section 27.1 of PIPEDA prohibits an employer from taking any adverse action toward an employee who:

- discloses to the Commissioner that the employer has contravened or intends to contravene PIPEDA,
- refuses to do anything that contravenes PIPEDA, or
- takes any action to prevent the contravention of PIPEDA.

This provision appears broad enough to adequately protect employees. However, one area that might be broadened is extending the protection to *any* person who reports a contravention of the privacy legislation.

RECOMMENDATION:

The National Privacy and Access Law Section of the Canadian Bar Association recommends that a provision be added to parallel similar protection to complainants under the *Canadian Human Rights Act*, for example, "prohibiting any person from threatening, intimidating or discriminating against an individual because that individual has made a complaint, given evidence or assisted in the initiation or prosecution of a complaint under the Act."

VIII. CONSENT ISSUES

A. Express vs. Implied Consent

Under PIPEDA, the sensitivity of the information at issue drives the form of consent required. Where the information is more sensitive, express consent is required. However, while sensitivity is a factor, the model for consent adopted by B.C. and Alberta PIPAs is that deemed and implied consent may be sufficient where enumerated criteria are met.

RECOMMENDATION:

The National Privacy and Access Law Section of the Canadian Bar Association recommends that PIPEDA adopt a two-part approach as in sections 7(1) and 8 of B. C. PIPA, so an individual provides implied consent where:

- **the purposes would be considered obvious to a reasonable person, and the individual voluntarily provides the personal information to the organization for that purpose; or**
- **the individual is provided with information as to the purposes, the individual has the opportunity to decline but does not do so, and the collection, use and disclosure is reasonable having regard to the sensitivity of the personal information in the circumstances.[23]**

B. Third Party Consent

There are circumstances where consent is not obtained directly from a person whose personal information is being collected, used or disclosed. For example, an applicant for a loan may be asked to provide certain personal information about their spouse and to indicate that the spouse's consent has been obtained. While in some circumstances, the person communicating the consent to the entity could be considered the other individual's agent, this would not always be the case.

RECOMMENDATION:

The National Privacy and Access Law Section of the Canadian Bar Association recommends that PIPEDA address the issue of consent obtained indirectly from an individual through another person. An organization should be permitted to rely, acting reasonably, on an assurance or on surrounding circumstances that a person providing personal information of another individual has consent of the other individual for the specific purposes involved, or that the other individual would

23 See sections 7 and 8(3) of the B.C. statute.

consent if aware of the circumstances (a donation or gift). Factors in assessing the reasonableness of this reliance include the nature of the transaction, the sensitivity of the personal information, whether the collection, use or disclosure benefits the individual, the nature of the relationship between the individual and the person confirming the individual's consent, and apparent authority given by one individual to deal with another individual, and should be explicitly listed, although the list need not be exhaustive.

C. Consent By Minors

Principle 4.3.6 allows an authorized representative, such as a legal guardian, to provide consent. It is unclear, however, whether a minor (as defined by statute) can ever give consent personally. Can minors, for example, consent to participate or enter contests, promotions, or other on-line activities? It should be clarified that minors can in fact consent if they understand the nature of their action and the consequences of giving consent. Consideration should also be given to stipulating a minimum age below which consent may not be given, such as contained in the Canadian Marketing Association guidelines regarding marketing to children and teenagers and the U.S. *Children's Online Privacy Protection Act*. Those rules provide a stipulated minimum age (13 years) below which consent must be given by a parent. At present, PIPEDA's only rule respecting substitute consent requires consent by a legal guardian, which in most provinces does not necessarily mean a parent, or by a power of attorney. Both are impractical in most situations involving any requirement for consent by young children.

RECOMMENDATION:

The National Privacy and Access Law Section of the Canadian Bar Association recommends that PIPEDA be amended to provide that minors may consent to the collection, use and disclosure of their personal information if they understand the

nature of giving consent and its consequences, and provided that below a certain age (for example, 13 years) such consent must be given by a parent or legal guardian.

D. Contingent or Tied Consent

The prohibition on contingent or tied consent in Principle 4.3.3 uses the term, "required to fulfil the explicitly specified, and legitimate purposes" that is inconsistent with the wording elsewhere in PIPEDA. This is unnecessarily confusing.

RECOMMENDATION:

The National Privacy and Access Law Section of the Canadian Bar Association recommends that Principle 4.3.3 be re-written to use the same "reasonableness" language used elsewhere in PIPEDA, and that a list of factors for determining the reasonableness of contingent consent be provided. This Principle should also be clarified to specify whether the proposed use of the personal information must be directly related to the purposes for which information is collected, or whether secondary uses are permitted if clearly identified and consent has been provided.

IX. DISCLOSURES OUTSIDE OF CANADA (OUTSOURCING)

A. Application and Rules - Possible Prohibition/Notification Required for Processing and Storing Personal Information outside of Canada

The Privacy Commissioner of Canada has stated that the legislative review of PIPEDA in 2006 would be a forum for developing further privacy protection measures related to trans-border information-sharing by the private sector. An indication of one such measure can be found in her submission to the British

Columbia Privacy Commissioner, concerning the impact of the U.S. *Patriot Act* on the personal health information of B.C. residents. The submission states that, "at the very least," a company in Canada that out-sources information processing to organizations based abroad should notify its customers that the information may be available to the foreign government or its agencies under a lawful order made in that country. It also encourages individuals to file complaints with her office if they are concerned about their personal information being held in databases outside Canada. Similarly, the British Columbia Commissioner's report ultimately recommended that the provincial and federal governments consider and address the implications of the *USA Patriot Act* for the security of personal information in respect of private sector activities.

The issue of trans-border transfer of information is specifically addressed in section 16 of the Quebec Act. The section obliges persons "communicating" information about Quebec residents to persons outside the province to take all reasonable care to ensure that it is not disclosed to third parties without consent, except as provided in the legislation.

British Columbia recently enacted Bill 73 to amend the public sector privacy legislation (the *Freedom of Information and Protection of Privacy Act* or FOIPPA) to address concerns about possible unauthorized disclosures of personal information to U.S. authorities by "U.S.-linked entities" pursuant to the *Patriot Act*. To summarize the most significant amendments:

- Storage only in Canada: Public sector entities, and their service providers, are now required to ensure that personal information in their custody or control is stored, and accessed, only in Canada, unless (a) the individual the information is about has "identified" the information and has consented, in the prescribed manner, to it being stored in or accessed from another jurisdiction, or (b) if it is stored in or accessed by another jurisdiction for the purpose of disclosure allowed under FOIPPA;
- Reporting of all Foreign Demands for Disclosure: Public bodies and their service providers are now required to report to the Minister responsible for FOIPPA all actual or suspected "foreign demands for

disclosure" (defined as a foreign subpoena, warrant, order, demand or request from a foreign authority, for disclosure not otherwise authorized by FOIPPA); and

- Prohibition of Disclosure in response to Foreign Demands for Disclosure: Public bodies and their service providers are now required to refuse to comply with foreign demands for disclosure.

During the same time period, the federal Treasury Board of Canada Secretariat (TBS) requested that the Access to Information and Privacy Coordinators for various federal institutions conduct a comprehensive audit of the outsourcing activities of such institutions to the extent that they involved the handling of personal information of Canadians and other sensitive data "to identify, assess and, if appropriate, mitigate any possible risks related to the *Patriot Act*". Concurrently, TBS is leading a working group to finalize "Privacy Model Clauses" regarding the *Patriot Act* for future Requests For Proposals and contracts. In their January 2005 *Information Notice*, TBS estimated that the Privacy Model Clauses would be made available in February 2005. We understand that TBS is finalizing such clauses with the federal office of the Privacy Commissioner, and that model clauses are expected within the next several weeks.

If the Office of the Privacy Commissioner is considering restricting the storage and/or processing of personal information outside the country by private sector entities, the following questions arise:

a. Should an organization be required to provide notice, or obtain consent, where personal information is to be processed or stored outside of Canada?
b. Should it make any difference if the jurisdiction in which the information is to be stored and processed has stringent privacy rules (for example, in the UK under the *Data Protection Act*)?

Section 17 of Quebec PPIPS deals with personal information relating to Quebec residents being entrusted to persons outside of Quebec:

> 17. Every person carrying on an enterprise in Quebec who communicates, outside Quebec, information relating to persons residing in Quebec or entrusts a person outside Quebec with the task of holding, using or communicating such information on his behalf must take all reasonable steps to ensure
>
> > 1) that the information will not be used for purposes not relevant to the object of the file or communicated to third persons without the consent of the persons concerned, except in cases similar to those described in sections 18 and 23;
> >
> > 2) in the case of nominative lists, that the persons concerned have a valid opportunity to refuse that personal information concerning them be used for purposes of commercial or philanthropic prospection and, if need be, to have such information deleted from the list.

Under PIPEDA currently, information processed by a third party processor for an organization is considered to still be in the custody and control of that organization; the organization must ensure that such information is protected through contractual or other measures; and the organization remains responsible for protecting the information. The only additional protection for processing and/or storage extra-jurisdictionally is that the individual will have the opportunity to refuse to consent to have his or her information processed or stored outside of Canada.

Were an individual to refuse consent, the organization would be justified in either:

- refusing to provide the service where a reasonably cost-effective alternative is not available, or
- where a reasonably cost-effective alternative mechanism is available, providing such alternative mechanism, but charging the individual for any additional incremental costs in relation to same.

However, having two different means of processing and storing data - one outside of Canada (to take advantage of cost savings, for example) and one inside Canada only for those individuals who do not want to have their information stored or processed outside of Canada, may well be impractical for an organization to implement.

B. Trigger for, and Content of, Notice for Extra-Jurisdictional Processing and Storing

The most significant issues are the appropriate trigger for any notification/consent requirement, and the amount of detail required for such notice. We canvas some possible options below.

Option 1: Identifying that information may be made available to public authorities

Canada's Privacy Commissioner has suggested that, at the very least, a company in Canada that out-sources information processing to organizations based abroad should notify its customers that the information may be available to the foreign government or its agencies under a lawful order made in that country. The problem is that there is no way for an individual to be alerted to the fact that such information would also be available under lawful orders made in *any* country, or that such information may be available under lawful orders *in Canada*.

Option 2: Identifying that information may be made available to public authorities in specified circumstances where it would not be in Canada

If the function of the notice is to caution the individual as to the existence of an additional risk not found in Canada, then the notice should identify that specifically. While perhaps providing more value to the individual than the broader statement suggested by the Privacy Commissioner, this model also raises certain problems:

- An organization that contemplates processing or storage in another country would have to retain local counsel to provide an opinion either that there is no greater risk of disclosure to public authorities under the laws of the local jurisdiction, relative to Canada (which, as such opinion would be based on a comparative law analysis, would be a difficult opinion to provide), or that there is an additional risk of disclosure, specifically which additional risks are present. If counsel can identify those additional risks, such risks would assumedly be summarized in the notice/consent so that the individual could be fully informed in making their decision.

- The extent of the risk involves an inherently qualitative assessment, which is often difficult to make. The risk would be the product of an assessment of the laws in the local jurisdiction that provide public authorities with more intrusive powers to require disclosure of personal information than in Canada, multiplied by the probability that those powers will actually be exercised by local authorities.

Under the *European Data Directive*, of course, the existence of (a) the adequacy principle, wherein personal information may be disclosed outside of a EU member state only[24] where the recipient country has adequate privacy protections, and (b) a list of countries which have been determined by the EU to meet this principle, allows organizations to omit such an assessment. The challenge is that the list of countries found to meet the adequacy principle is very short.

Option 3: Identifying the specific country in which the personal information will be processed or stored.

This relieves the organization of the burden of assessing the specific, incremental risks of storing/processing in a particular jurisdiction, but shifts the burden of assessing the risks to each individual. However, identifying the specific country also restricts the organization from later moving the location of storage or processing to another country without obtaining a new consent or providing a new notice.

Option 4: Identifying the specific country in which the personal information will be processed or stored, only where that country does not have adequate privacy protections re preventing disclosures to public authorities, as determined by Industry Canada

This option would give Industry Canada the burden of assessing which country has inadequate protections regarding public authorities. Where personal information is to be processed or stored in, for example, a member state of the EU that has implemented the European Data Directive, or that has been found adequate by the EU, the organization may not need to identify the country on the

24 Subject to the model contract clauses, and the U.S. safe harbour regime.

notice/consent. One of the major problems of the amended FOIPPA preventing storage or processing outside the country without consent, is that, unlike the European Data Protection Directive, it draws no distinction between processing in a country that has implemented the Directive, such as the U.K., and a country with few or no personal information protection laws, such as India. As with Option 3, identifying a specific country again restricts the organization from later moving the location of storage or processing to another country, without obtaining a new consent or providing a new notice.

C. Summary

The notification options outlined above demonstrate the complexities of disclosing the use and storage of personal information outside of Canada, and the many challenges that disclosure presents.

We note that each organization remains responsible for the personal information in its custody and control in any case. As an alternative to, or in addition to these proposals, additional language regarding the security of Canadian personal information could be added to contracts between organizations and entities storing or processing the personal information for the organization. Section 8(4) of Alberta Regulation 70/2001 of the *Alberta Health Information Act* is an example of such a provision:

> In order to ensure the privacy and confidentiality of health information that is to be stored or used by a person in a jurisdiction outside Alberta or that is to be disclosed to a person in a jurisdiction outside Alberta, the custodian must, prior to the storage, use or disclosure of the information, enter into a written agreement with the person that
>
> (a) provides for the custodian to retain control over the health information,
>
> (b) adequately addresses the risks associated with the storage, use or disclosure of the health information,

(c) requires the person to implement and maintain adequate safeguards for the security and protection of the health information,

(d) allows the custodian to monitor compliance with the terms and conditions of the agreement, and

(e) contains remedies to address any non-compliance with or breach of the terms and conditions of the agreement by the other person.

RECOMMENDATION:

The National Privacy and Access Law Section of the Canadian Bar Association recommends that where personal information is to be stored or processed in a jurisdiction outside Canada, PIPEDA require additional provisions in contracts between organizations and entities storing or processing personal information for organizations, to enhance security of the personal information and ensure conformity to Canadian law.

X. CONCLUSION

The National Privacy and Access Law Section appreciates the opportunity to provide input about issues for consideration during the upcoming review of PIPEDA at this preliminary stage. We trust that our comments will be helpful, and look forward to participating further in the future.

Privacy Rights in Canada

WHEREAS the Supreme Court of Canada has recognized privacy as a fundamental value of Canadian society;

WHEREAS privacy is fundamental to the dignity and autonomy of the person;

WHEREAS in numerous submissions to Parliament and to Government departments, the Canadian Bar Association has urged restraint, balance and accountability when infringements of privacy and civil rights are proven essential for legitimate public objectives;

WHEREAS the Canadian Bar Association recognizes that governments and organizations have certain legitimate reasons to collect, use and disclose personal information for limited purposes, and that individuals have the right to access their own information as retained by governments and organizations;

BE IT RESOLVED THAT the Canadian Bar Association confirm its strong commitment to preserving, promoting and respecting privacy by:

Droits de la protection des renseignements personnels au Canada

ATTENDU QUE la Cour suprême du Canada a reconnu la vie privée comme une valeur fondamentale de la société canadienne;

ATTENDU QUE la vie privée est essentielle à la dignité et à l'autonomie de la personne;

ATTENDU QUE dans plusieurs mémoires adressés au Parlement et aux ministères du gouvernement, L'Association du Barreau canadien a insisté sur l'importance de veiller à la restriction, à l'équilibre et à la responsabilité lorsque des atteintes à la vie privée et aux droits civils sont jugées essentielles pour justifier des objectifs publics légitimes;

ATTENDU QUE L'Association du Barreau canadien reconnaît que les gouvernements et organisations ont parfois des raisons légitimes de recueillir, d'utiliser et de divulguer des renseignements personnels à des fins limitées et que les personnes ont le droit d'accéder aux renseignements qui les concernent et qui sont détenus par des gouvernements et organisations;

QU'IL SOIT RÉSOLU QUE L'Association du Barreau canadien réitère son ferme engagement à préserver, promouvoir et respecter la vie privée en :

1. encouraging its National and Branch organizations to be vigilant in monitoring and opposing unnecessary erosions of privacy by both government and non-governmental organizations;

2. calling on other professional associations, industry, academia, labour, governments and the public to work together to preserve, promote and respect privacy in Canada and worldwide; and

3. urging governments to better preserve, promote and respect privacy, and specifically to:

   (a) ensure that the collection, use and disclosure of personal information, without knowledge and consent, is conducted in a manner that is reasonable and necessary in the circumstances and that any exceptions to such collection, use and disclosure be express and clearly stated;

   (b) promote and foster fair information principles set out in the *Model Code for the Protection of Personal Information*, including the right of access and accountability,

   (c) ensure that the need of government to collect, use and disclose personal information in relation to national security and law enforcement are subject to reasonable and attainable objectives and

1. encourageant ses entités nationales et divisionales à surveiller de près toute forme d'atteinte à la vie privée de la part d'organisations gouvernementales et non gouvernementales et à s'y opposer lorsqu'il y a lieu;

2. demandant à d'autres organisations professionnelles, à l'industrie, au milieu universitaire, aux syndicats, aux gouvernements et au public de collaborer afin de préserver, de promouvoir et de respecter la vie privée au Canada et dans le reste du monde; et

4. exhortant les gouvernements à préserver, à promouvoir et à respecter davantage la vie privée et, en particulier, à :

   (a) veiller à ce que la collecte, l'utilisation et la divulgation des renseignements personnels, à l'insu des personnes visées et sans leur consentement, soient effectuées de manière raisonnable et nécessaire dans les circonstances et que toute exception à ces collecte, utilisation et divulgation soit expressément et clairement énoncée;

   (b) promouvoir et favoriser l'adoption de principes justes en matière de renseignements personnels dans le *Code type sur la protection des renseignements personnels*, notamment le droit d'accès et la responsabilité;

   (c) veiller à ce que le besoin du gouvernement de recueillir, utiliser et divulger les renseignements personnels à des fins de la sécurité nationale et du contrôle d'application des lois soient assujetés à des

respect the privacy of individual Canadians to the maximum extent possible, having due regard to the right of individual Canadians to security of the person and to the benefit of the rule of law;

(d) provide sufficient resources to enable proper enforcement of its privacy legislation and enhancement of awareness of individuals and organizations of their rights and obligations with respect to personal information;

(e) encourage the harmonized development of privacy legislation, policies and practices throughout Canada; and

(f) encourage privacy commissioners across Canada to work together to produce uniform interpretations, policies and procedures to provide needed guidance to individuals and organizations.

objectifs raisonnables et atteignables et respectent le plus possible la vie privée des Canadiens et Canadiennes, en tenant compte de leur droit de sécurité personnelle et des avantages de la règle de droit;

(d) allouer des ressources suffisantes pour permettre l'application adéquate de la législation sur la protection des renseignements personnels et faire davantage connaître aux individus et organisations leurs droits et obligations vis-à-vis des renseignements personnels;

(e) encourager l'harmonisation entre les différentes lois, politiques et pratiques des lois sur la protection des renseignements personnels dans l'ensemble du Canada;

(f) inciter les commissaires à la protection de la vie privée dans l'ensemble du Canada à collaborer en vue d'adopter des interprétations, des politiques et procédures uniformes fournissant aux individus et aux organisations l'orientation nécessaire.

Certified true copy of a resolution carried by the Council of the Canadian Bar Association at the Annual Meeting held in Winnipeg, MB, August 14-15, 2004.

Copie certifiée conforme d'une résolution adoptée par le Conseil de l'Association du Barreau canadien, lors de son Assemblée annuelle, à Winnipeg (MB), les 14 et 15 août 2004.

John D.V. Hoyles
Executive Director/Directeur exécutif

OFFICE OF THE PRESIDENT
CABINET DU PRÉSIDENT

July 5, 2006

The Hon. Vic Toews, P.C., M.P.
Minister of Justice and Attorney General of Canada
House of Commons
Ottawa ON K1A 0A6

The Hon. Stockwell Day, P.C., M.P.
Minister of Public Safety
House of Commons
Ottawa ON K1A 0A6

The Hon. Maxime Bernier, P.C., M.P.
Minister of Industry
House of Commons
Ottawa ON K1A 0A6

Dear Ministers,

I write on behalf of the Canadian Bar Association (CBA) concerning a trend by internet service providers (ISPs) to monitor or investigate their customers' communications, similar to proposals in Bill C-74 from the 38th session of Parliament, the *Modernization of Investigative Techniques Act* (the Bill). The CBA is a national professional organization representing over 36,000 lawyers, notaries, law students and teachers from every part of Canada. The CBA's mandate includes seeking improvements in the law and the administration of justice, and being the voice of the Canadian legal profession.

The CBA is concerned that ISPs are amending their service agreements with customers to announce that they will "monitor or investigate" how customers use their services, and will "disclose any information necessary to satisfy any laws, regulations or other governmental request from any applicable jurisdiction." This seems to be introducing a corporate or industry content monitoring scheme, without the necessity of prior authorization or oversight. This initiative appears significantly more intrusive than the previous legislative proposal.

In consultations about so-called "lawful access", government officials characterized proposals as simply updating current law enforcement powers to recognize technological realities. The CBA voiced strong concerns about the scope and potential impact of the

500 - 865 Carling, Ottawa, Ontario Canada K1S 5S8
Tel/Tél. : (613) 237-2925 Toll free/Sans frais : 1-800-267-8860 Fax/Télécop. : (613) 237-0185
Home Page/Page d'accueil : www.cba.org E-Mail/Courriel : info@cba.org

various proposals. Our concerns focus on the profound impact on the privacy of individual Canadians, and particularly on the potential to destroy solicitor client privilege by seizing communications between lawyers and clients. Solicitor client privilege is a cornerstone of democracy and the Canadian legal system. It allows individuals to seek legal advice knowing that communications with their counsel will remain private, and protected by law. Solicitor client privilege belongs to the individual seeking legal advice and is for the benefit of the client, not the lawyer.

In our view, all "lawful access" measures must be defined to conform with legal protections and guarantees that safeguard Canadians' rights and freedoms, and be closely monitored to ensure that conformity. Prior judicial authorization is central, and blanket customer agreements without prior judicial authorization or oversight do not meet that test. A heightened level of care and scrutiny is imperative where the interception or search of such communication may infringe solicitor client privilege.

We urge you to ensure that Canadians' private information remains appropriately protected, and that any privilege accorded to communications between lawyers and clients remains inviolate. We would appreciate an opportunity to discuss this with you or your officials at greater length.

Yours truly,

(Original signed by Brian A. Tabor)

Brian A. Tabor, Q.C.