HOUSE OF COMMONS
CANADA

STATUTORY REVIEW OF THE PERSONAL INFORMATION PROTECTION AND ELECTRONIC DOCUMENTS ACT (PIPEDA)

Fourth Report of the Standing Committee on Access to Information, Privacy and Ethics

Tom Wappel, MP
Chairman

May 2007

39th PARLIAMENT, 1st SESSION

Also available on the Parliamentary Internet Parlementaire: http://www.parl.gc.ca

Available from Communication Canada — Publishing, Ottawa, Canada K1A 0S9

STATUTORY REVIEW OF THE PERSONAL INFORMATION PROTECTION AND ELECTRONIC DOCUMENTS ACT (PIPEDA)

Fourth Report of the Standing Committee on Access to Information, Privacy and Ethics

Tom Wappel, MP
Chairman

May 2007

39th PARLIAMENT, 1st SESSION

STANDING COMMITTEE ON ACCESS TO INFORMATION, PRIVACY AND ETHICS

CHAIRMAN

Tom Wappel

VICE-CHAIRMEN

Pat Martin

David Tilson

MEMBERS

Sukh Dhaliwal

Glen Pearson

Scott Reid

Dave Van Kesteren

Mike Wallace

Carole Lavallée

Jim Peterson

Bruce Stanton

Robert Vincent

CLERK OF THE COMMITTEE

Richard Rumas

LIBRARY OF PARLIAMENT

Parliamentary Information and Research Service

Kristen Douglas

Nancy Holmes

THE STANDING COMMITTEE ON ACCESS TO INFORMATION, PRIVACY AND ETHICS

has the honour to present its

FOURTH REPORT

Pursuant to its mandate under Standing Order 108(2), the Committee has studied a Statutory Review of the Personal Information Protection and Electronic Documents Act (PIPEDA) and agreed to the following report:

TABLE OF CONTENTS

INTRODUCTION

Pursuant to section 29 of the *Personal Information Protection and Electronic Documents Act* (PIPEDA) and an order of the House of Commons, the Standing Committee on Access to Information, Privacy and Ethics (the Committee) held hearings on the administration of Part 1 of the Act, Protection of Personal Information in the Private Sector. The Committee heard from 67 witnesses between November 20, 2006 and February 22, 2007 and received 34 submissions from additional individuals and organizations.

All of our witnesses were generally supportive of a federal private sector data protection law, particularly in view of the rapidly expanding myriad of information technology and its ability to transcend national borders. In this context, the crux of the debate before us was how best to maintain the balance sought by the legislation in terms of protecting the privacy rights of individuals (what is known about them and by whom) and the legitimate needs of business organizations to manage their information holdings.

This report does not advocate dramatic changes to PIPEDA at this time. Given that the full implementation of the Act did not come about until January 2004 (see Overview of the Act, below), the Committee is cognizant of the fact that not every aspect of its implementation has yet been fully realized. Thus, even though we heard arguments on numerous issues, we have addressed only those where we decided that comments are warranted at this time.

The recommendations in this report essentially seek to provide some fine-tuning, much of which is premised on the need for greater harmonization between PIPEDA and the provinces of Quebec, Alberta and British Columbia, all of which have substantially similar private sector data protection laws. Indeed, we heard from privacy advocates, academics, business and industry organizations, as well as from the Federal Privacy Commissioner, that reference should be made to these provincial laws when making changes to PIPEDA. In particular, it was argued that the Alberta and British Columbia laws, having been drafted subsequent to the Quebec and federal Acts, have had the benefit of drawing upon the Quebec and federal experiences and incorporating enhancements to their legislation. It was argued that these “second generation” privacy laws provide a more practical and updated reflection of privacy protection today.

We recognize that there is a need to devote more resources to the education of both individuals and organizations about their respective rights and responsibilities under PIPEDA. We heard evidence that most Canadians are unaware of their privacy rights in general, let alone those with respect to PIPEDA. We also heard that one of the biggest challenges for most small and medium businesses is to understand their obligations under the law. In our view, the success of any amendments we propose to PIPEDA, and ultimately of PIPEDA itself, will depend on individuals being able to make informed choices

about their personal information and organizations being fully aware of their obligations under the Act. Given that the Office of the Privacy Commissioner has a clear mandate to foster public awareness and encourage compliance amongst organizations subject to the legislation, we hope that more work will continue to be done in this area and that the government, for its part, will also work with both organizations and the Privacy Commissioner to this end.

OVERVIEW OF THE ACT

Subject to certain statutory exemptions,[1] PIPEDA applies to private sector organizations that collect, use or disclose personal information in the course of commercial activities. It also applies to the collection, use and disclosure of personal information pertaining to the employees of federally regulated organizations.[2] Personal information is broadly defined (section 2(1)) as "information about an identifiable individual, but does not include the name, title or business address or telephone number of an employee of an organization." Obviously intending to capture a broad range of transactions, section 2 of PIPEDA defines "commercial activity" 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."[3]

PIPEDA has come into effect in three stages:

- On January 1, 2001, the Act applied only to the federally regulated private sector (i.e., telecommunications, broadcasting, banking and interprovincial transportation and airline industries). It also covered interprovincial or international trade in personal information.

- On January 1, 2002, personal health information became subject to the Act.

---

1 The Act does not apply to any government institution to which the federal *Privacy Act* applies; to personal information collected, used or disclosed by an individual exclusively for personal or domestic purposes; or to organizations in respect of personal information that is collected, used or disclosed for journalistic, artistic or literary purposes (s. 4(2)).

2 Notwithstanding provincial jurisdiction over labour relations, the federal government can regulate employee information but only in relation to works, undertakings and businesses that are within the legislative authority of the federal Parliament.

3 PIPEDA is limited in its scope to commercial activities because the provinces have exclusive jurisdiction over matters of private property and civil rights. The federal government therefore chose to regulate this area based on its general power to regulate trade and commerce.

- On January 1, 2004, the provisions of the Act extended more broadly to include all organizations located entirely within a province, even if they collect, use or disclose personal information only within that province. Where, however, a province enacts legislation that is substantially similar to the federal law, organizations covered by the provincial legislation may be exempted from the application of the federal Act. To date, only Quebec, Alberta, Ontario (with respect to personal health information) and British Columbia have provincial legislation that has been accorded the status of substantially similar to PIPEDA.

Once an organization falls within the scope of PIPEDA, section 5 requires that it comply with the fair information obligations set out in the Canadian Standards Association (CSA) Model Code (Schedule 1 of the Act)[4], unless the exceptions contained in sections 6 to 9 apply. Section 5 also provides that the use of the word "should" in Schedule 1 indicates a recommendation and does not impose an obligation. Section 5(3) of the Act further stipulates a "purposes" test by stating that the purposes for which an organization can collect, use or disclose personal information are to be limited to those that "a reasonable person would consider are appropriate in the circumstances." Section 7 of the Act sets out a number of exemptions pursuant to which an organization can collect, use or disclose personal information without the knowledge or consent of the individual and as such, is critical to the operation of the Act's privacy regime.[5]

PIPEDA provides individuals with a right to have access to their personal information and to have it corrected, if necessary. An organization must respond to a request for access within 30 days, but can extend this time limit under certain conditions; it can refuse to give an individual access to his or her personal information where this would reveal personal information about a third party and the third-party information cannot be severed from the record. If the third party consents, however, or if the individual needs the information because his or her life, health or security is threatened, the third-party prohibition will not apply. Furthermore, an organization can refuse to give access to

---

[4] In response to the lack of national data protection standards in Canada in the early 1990s, a committee of consumer, business, government and labour representatives developed, under the auspices of the Canadian Standards Association (CSA), a set of privacy protection principles that, in 1996, were approved as a national standard by the Standards Council of Canada. The CSA *Model Code for the Protection of Personal Information* comprises ten interrelated privacy principles that were designed to serve as a fair information practices guide that could be adopted by businesses. The text of the CSA Code was ultimately incorporated into PIPEDA as a Schedule to the Act. For more on the origins of the Code and its adoption into PIPEDA, see *The Personal Information Protection and Electronic Documents Act: An Annotated Guide* by Perrin, Black, Flaherty and Rankin, Irwin Law Inc., Toronto, 2001.

[5] For example, personal information may be *collected* without the knowledge or consent of an individual for law enforcement purposes; when the collection is in the best interests of the individual; when the collection is for journalistic, artistic or literary purposes; or where the information is publicly available. Personal information may be *used* without the knowledge or consent of an individual for similar reasons, as well as for research purposes in certain instances with the knowledge of the Privacy Commissioner. Finally, personal information may be *disclosed* without the knowledge or consent of the individual for law enforcement and national security purposes, emergency situations, as well as research or archival purposes.

personal information where the information is protected, for example, by solicitor-client privilege or where access to the information would reveal confidential commercial information.[6] Access is permitted, however, if the individual needs the information because his or her life, health or security is threatened.

PIPEDA is administered pursuant to an ombudsman model similar to that found in the *Privacy Act* and the *Access to Information Act*. Individuals may complain to the Federal Privacy Commissioner about an organization's compliance with the legislation or the CSA Code[7], and the Commissioner will usually attempt to resolve the matter through persuasion and negotiation. Where this approach does not work, the Commissioner has the power to summon witnesses, administer oaths and compel the production of documents in order to render a finding in the matter. This finding must be set out in a report by the Commissioner within one year of the filing of the complaint. The Commissioner's findings are not binding on the parties, nor do they have persuasive value before the Federal Court. The complainant, after receiving the Commissioner's report, does however have the right to seek judicial remedies, including orders to comply and damages, from the Federal Court.

The Privacy Commissioner also has the power, under section 11 of the Act, to initiate her own complaints when she is satisfied that there are reasonable grounds to investigate a matter under the law. The Commissioner may apply to the Federal Court for review of complaints she has initiated as well as on behalf of a complainant with his or her consent. Pursuant to section 18 of the Act, the Privacy Commissioner also has the power to audit the personal information management practices of an organization where the Commissioner has reasonable grounds to believe that the organization is contravening the provisions of the legislation pertaining to the protection of personal information, or is not following a recommendation set out in the CSA Model Code.

Section 28 of PIPEDA creates offences for obstructing the Commissioner in an investigation or an audit, destroying records that are the subject of an access request before all recourse under the Act is exhausted, or dismissing, suspending, or demoting an employee who discloses a violation of the Act by his or her employer.

---

6 These access exemptions largely mirror those found in the *Access to Information Act* and are an example of the complementary nature of the privacy and access regimes.

7 Section 11.

DEFINITIONS

1. Personal Information

A. Business Contact Information

Section 2(1) of PIPEDA defines "personal information" for the purposes of the Act as "information about an identifiable individual, but does not include the name, title or business address or telephone number of an employee of an organization." Thus, business contact information is excluded from privacy protection in order that customers and others can easily communicate with the employees of organizations. Similar provisions are found in the federal *Privacy Act* with respect to public servants.

We heard from several organizations that the exclusion of business contact information under the Act should be broadened in order to recognize the current realities of how businesses communicate with their customers. It was suggested that a definition of "business contact information" be included in the Act to include all relevant types of information that are given out in a business context, and that the definition not be tied to any specific technology. Thus, business contact information should include business email and fax numbers as well as other similar business information.

The Privacy Commissioner directed the Committee's attention to the approach taken in the Alberta *Personal Information Protection Act*. The Commissioner liked the definition in this second general privacy law because it is sufficiently broad, but it also places restrictions on the purposes for which such information may be collected, used or disclosed.

Section 1(a) of the Alberta Act defines "business contact information" as an "individual's name, position name or title, business telephone number, business address, business email, business fax number and other similar business information." Section 4(3)(d) of the Act is the exception provision that states that the Act does not apply to business contact information where it is collected, used or disclosed for the purposes of contacting an individual in that individual's capacity as an employee or an official of an organization, and for no other purpose.

This Committee feels that business contact information should be excluded from PIPEDA's privacy protections and that what constitutes such information should not be tied to the information technology that exists at a particular point in time. The Act should therefore be updated to include business email and fax numbers, as well as future innovations in business communication. Like the Privacy Commissioner, we prefer the Alberta approach to this issue and make the following recommendation.

Recommendation 1

The Committee recommends that a definition of "business contact information" be added to PIPEDA, and that the definition and relevant restrictive provision found in the Alberta *Personal Information Protection Act* be considered for this purpose.

B. Work Product

The distinction between what is personal information about an individual, as opposed to information generated as a result of professional, business or employment activity, and its explicit recognition in PIPEDA, was a point raised by employers, businesses and health information providers. Many businesses are concerned about the effect on innovation and economic growth if workers are able to treat data about their work output or business strategies as personal information under PIPEDA. Mark Yakabuski, of the Insurance Bureau of Canada, put it this way:

> In a competitive economy — and I know that Parliament wants a competitive economy — it is absolutely essential that companies have access to information about the products and services that they in turn buy from other businesses, so that they can use this information to innovate and improve the products and service they sell their customers. Without access to work product information, innovation and competition will be stifled in the economy. (February 6, 2007)

There was a great deal of support from businesses for the approach taken by the British Columbia *Personal Information Protection Act*, which defines work product information as distinct from personal information under the Act. Section 1 of the B.C. law defines "work product information" as "information prepared or collected by an individual or group of individuals as a part of the individual's or group's responsibilities or activities related to the individual's or group's employment or business, but does not include personal information about an individual who did not prepare or collect the personal information." Most businesses support this definition because they believe it would provide certainty by allowing for consistent application.

In his brief to the Committee, the Information and Privacy Commissioner for British Columbia, David Loukidelis, noted that difficulties in interpretation and application can arise if a privacy law does not distinguish between personal information that is about someone as an individual and information they produce or compile as part of their work or business duties or activities. Interestingly, however, he had this to say when questioned by Committee members about the issue:

> As I mentioned, in British Columbia's law we have a definition of "work product information", and clearly the legislature, using specific language, has given me direction. It's my obligation, on a case-by-case basis, if the matter actually comes to me in a formal inquiry, to interpret and apply those words as intended by the legislature. Having said that, if we didn't have that definition, and if in fact we were to fall back on a definition of

> "personal information", which is "information about an identifiable individual", you would still have the same opening that has been taken here by my federal colleagues and in other provinces under their public sector legislation to try to interpret what information is "about" an individual in the sense intended by the legislature, and perhaps coming to the same result that has to be said. (November 29, 2006)

The issue of "work product" was of particular significance in relation to health information. IMS Canada, a principal provider of information, statistical research and analysis to the health sector, sought a definition of "work product" that is similar to the B.C. approach, but which also attempts to address some of the Privacy Commissioner's concerns that workplace monitoring and surveillance might inadvertently get caught up in a broad definition or interpretation of the term. Although the Privacy Commissioner had already found that physician prescribing patterns, information of particular concern to IMS, were not personal information for the purposes of PIPEDA, IMS would like this decision codified for greater certainty. The specific wording proposed by IMS was as follows:

> "work product information" means information prepared, compiled or disclosed by an individual or group as part of the individual or group's responsibilities related to their profession, employment or business. It does not include:
>
> i) personal information about an identifiable individual who did not prepare, compile or disclose the information; or
>
> ii) information collected, used or disclosed for the purposes of workplace surveillance. (February 8, 2007, brief, p. 34)

In response to the specific issue of whether information on doctor's prescriptions constitutes work product under PIPEDA, the Canadian Medical Association (CMA) takes the position that this data, along with other practice information, is the personal information of the physician, and physicians have legitimate privacy concerns about the use of this information by third parties for commercial purposes. While the CMA recommended that PIPEDA be amended to include physician information as personal information, it also made reference to Quebec's *An Act Respecting the Protection of Personal Information in the Private Sector,* which requires regulatory oversight and gives individuals the right to opt out of the collection, use and disclosure of professional information.

The Quebec approach is considered something of a compromise in that it treats work product information with respect to professionals as something in-between personal and non-personal information. The Act allows for the disclosure of personal information on professionals about their professional activities without individual consent; however, this disclosure can only take place with the authorization and subsequent supervision of the Quebec Commission (in consultation with the relevant regulatory body). As well, the individual professional must have the opportunity to refuse to allow his or her information to be used for the disclosed purpose, and he or she must be regularly notified of the

intended uses of the information. The authorized recipient of the information must also report annually to the Commission on the implementation of the authorization, and the Commission must publish a list of authorized persons in his annual report.[8]

The Federal Privacy Commissioner consistently maintained throughout our hearings that this was not an easy issue to address; in other words, there is no quick fix or one clear model to follow. She would prefer to maintain the current definition of personal information and deal with questions of work product on a case by case basis. The Commissioner also submitted that adopting her proposed employee code under PIPEDA[9] would resolve many of the issues associated with work product in a manner that would not threaten other workplace privacy rights.

This Committee recognizes that the issue of work product is not sector-specific. It is a matter that cuts across the full realm of commercial and employment activities. The Committee believes that there is need for clarification within PIPEDA as to what is work product as opposed to personal information under PIPEDA. While we are reticent to recommend specific wording in such a contentious area, we recommend that consideration be given to the B.C. definition, the definition proposed by IMS, as well as the approach taken by Quebec with respect to professional information.

Recommendation 2

The Committee recommends that PIPEDA be amended to include a definition of "work product" that is explicitly recognized as not constituting personal information for the purposes of the Act. In formulating this definition, reference should be made to the definition of "work product information" in the British Columbia *Personal Information Protection Act,* the definition proposed to this Committee by IMS Canada, and the approach taken to professional information in Quebec's *An Act Respecting the Protection of Personal Information in the Private Sector.*

2. Destruction

Principle 5 of Schedule 1 of PIPEDA addresses the issue of retention of personal information. Essentially, personal information shall be retained by an organization only for so long as is necessary to fulfill the purpose for which it was collected. After the information has served its intended purposes, and been retained for any prescribed periods, it should be destroyed, erased or made anonymous in accordance with disposal policies maintained by the organization (Principle 4.5.3). Principle 7 of the Schedule imposes security

[8] An Act Respecting the Protection of Personal Information in the Private Sector, R.S.Q. c. P-39.1, s. 21.1.

[9] See Consent part of the report regarding employee/employer relationships.

safeguards on the destruction process, such that care must be used in the disposal or destruction of personal information to prevent unauthorized parties from gaining access to the information (Principle 4.7.5).

In its appearance before the Committee, the National Association for Information Destruction (NAID) proposed a number of recommendations to ensure safe information destruction, something the organization feels is not happening in enough cases. Indeed, Mr. Dave Carey of NAID provided the Committee with a number of examples in support of the need for information destruction requirements to be spelled out in legislation. He summed things up for the Committee in this way:

> On any given day, it would not take long to find personal information being discarded, intact and accessible to the public. Careless disposal in dumpsters or garbage bins is the obvious example. Keep in mind as well, however, that recycling alone is not safe information destruction. Documents may still remain intact and vulnerable to privacy breaches for extended periods of time before being recycled. Privacy protection is no longer simply a human rights issue. Violating the rights of others by casually discarding their personal information provides much of the feedstock for what has become a global epidemic of identity fraud. According to a study conducted in the United States, the vast majority of identity theft results from low-tech access to personal information such as dumpster diving. (February 8, 2007)

NAID therefore recommended that the following definition of "destruction" be added to PIPEDA:

> For the purposes of principle 4.5 of Schedule 1, destruction is defined as the physical obliteration of records in order to render them useless or ineffective and to ensure reconstruction of the information (or parts thereof) is not practical. Destroy is defined as the act of destruction. (NAID Canada, letter dated February 21, 2007)

In its submission to the Committee,[10] the Ontario Ministry of Government Services stressed the need for greater education for organizations in terms of the secure destruction of personal information. As a result of the prevalence of identity theft in this country, the Ministry recommended that the Privacy Commissioner enhance her guidance on this issue by providing greater specificity on the steps organizations should take to destroy paper records and electronic media to ensure personal information is permanently destroyed or erased in an irreversible manner.

The Committee agrees that the proper destruction of personal information is an integral component of any personal information protection regime. Indeed, the privacy safeguards built into PIPEDA could be undermined if there is no specific destruction requirement in the Act. We therefore recommend that a definition of "destruction" be added to PIPEDA that would provide guidance to organizations on how to properly

[10] December 2006, p. 8.

destroy both paper records and electronic media. We have considered the definition of destruction, both in *The Concise Oxford Dictionary*, 10th ed., and *Le Petit Larousse illustré 2002*, and we commend these definitions for consideration in this regard.

Recommendation 3

The Committee recommends that a definition of "destruction" that would provide guidance to organizations on how to properly destroy both paper records and electronic media be added to PIPEDA.

CONSENT

1. General Principles

Consent is the cornerstone of most data protection statutes and is no less so in PIPEDA. With very limited exceptions, the Act requires knowledge and consent for the collection, use and disclosure of personal information in the course of commercial activities. The consent principles are set out in Principle 3 of the *CSA Model Code for the Protection of Personal Information*, which forms Schedule 1 of the Act. The difficulty with these general principles seems to be in reconciling them in a manner that reflects commercial realities and, at the same time, provides adequate privacy protection for consumers.

Consumer representatives and privacy advocates who appeared before us argued that it is extremely difficult to use the language of a voluntary consensus-driven document (the CSA Model Code)[11] as a basis for legislation. They argue that the wording of the consent principles is too vague and thus subject to wide-ranging interpretations which does little to help clarify what is actually required under the law. In its brief to the Committee, the Public Interest Advocacy Centre provided these comments:

> Schedule 1 of PIPEDA contains a broadly-worded "Consent Principle." This principle provides a general framework for thinking about consent for privacy purposes in a commercial context; however, its language provides very little in the way of concrete assistance to businesses and consumers looking for a definitive statement of what consent is, what consent is required under the Act and how to obtain it.
>
> For instance, the Model code instructs that when it comes to obtaining consent, "the form of consent sought by an organization may vary, depending upon the circumstances and the type of information." Similarly, the Code instructs that "in obtaining consent the reasonable expectations of the individual are also relevant" and that "the way in which an organization seeks consent may vary, depending on the circumstances and the type of information collected." It is obvious that these consent provisions permit both the

[11] See footnote 4.

> organization and the individual to argue that any processes set-up to obtain consent are deficient, or sufficient, from the point of view of either the individual or the business. (October 23, 2006, p. 14)

Arguments were also raised that PIPEDA's vague consent provisions are contributing to a significant lack of compliance with the legislation. In a report released in April 2006[12], the Canadian Internet Policy and Public Interest Clinic (CIPPIC) surveyed 64 on-line retailers and found that most are not obtaining meaningful consent to secondary uses and disclosures of consumer information. CIPPIC felt that its findings not only indicated an incentive/compliance problem, but also a lack of understanding of the consent requirements under the Act. It therefore recommended that a definition of "consent" be added to the legislation or at least clear preconditions and criteria for each of the three forms of consent (express, implied, deemed/opt-out). Reference was made to both the Alberta and British Columbia private sector data protection laws, which set out requirements for valid consent. The Ontario Ministry of Government Services, in a submission dated December 2006, also supported the idea that PIPEDA be amended to define and distinguish between different forms of consent in order to clarify both the obligations of organizations and the privacy rights of consumers.

Organizations generally support the consent principles as set out in PIPEDA because they provide the flexibility necessary for operating a business. It is also felt that the Act allows both businesses and consumers the ability to judge when additional information is required in order to make consent meaningful, and as such, there is no need to amend PIPEDA in this respect. In its brief to the Committee, the Canadian Marketing Association (CMA) had this to say on the definition of consent under PIPEDA:

> There are three forms of consent, which are currently recognized in the marketplace and are fundamental to information-based marketing activities. These forms of consent are the internationally recognized standard of industry and are specifically outlined in the CSA Model Code and in Chapter 5 of the Statutes of Canada 2000. They are: positive or express (opt-in) consent when dealing with sensitive information; negative option (opt-out) consent for the use of information for marketing purposes or for the transfer of non-sensitive information to third parties; and, implied consent, which allows a business to communicate with its existing customers. As outlined earlier in this brief, for many years CMA members have had to follow these forms of consent in their interactions with consumers. These were also the forms of consent that were recognized in PIPEDA, its related regulations and the interpretative findings of the Privacy Commissioner. The CMA feels strongly that these current definitions and applications of the three forms of consent should not be altered. (December 4, 2006, p. 11)

[12] *Compliance with Canadian Data Protection Laws: Are retailers measuring up?* at http://www.cippic.ca/en/bulletin/compliance_report_06-07-06_(color)_(cover-english).pdf.

Although the Privacy Commissioner did not specifically address the issue of consent in her appearances before the Committee, she has issued a fact sheet on determining the appropriate form of consent under PIPEDA.[13] The document is intended to provide guidance to organizations by identifying the consent principles under the Act and providing illustrations of how they have been interpreted and applied by the Office of the Privacy Commissioner.

While the Committee appreciates the concerns raised by consumer and privacy advocates about the vagueness of the consent principles found in Schedule 1 of PIPEDA (the CSA Model Code), we are averse to making any changes to the CSA Model Code portion of the Act given the enormous amount of consultation that went into crafting this standard, and the complexity of the compromises reached. That being said, we feel it is important that people have a clear understanding of the form and adequacy of consent required by PIPEDA. This is better set out in legislation than left to the Commissioner's guidelines or court decisions. We therefore recommend that consideration be given to clarifying in the legislation what is required for consent under PIPEDA and distinguishing between express, implied and deemed/opt-out consent. Reference should be made in this regard to the Alberta and British Columbia *Personal Information Protection Acts*.

Recommendation 4

The Committee recommends that PIPEDA be amended to clarify the form and adequacy of consent required by it, distinguishing between express, implied and deemed/opt-out consent. Reference should be made in this regard to the Alberta and British Columbia *Personal Information Protection Acts.*

2. Exceptions

A. Employee/Employer Relationship

As noted at the beginning of this report, PIPEDA is a law that establishes rules governing the collection, use and disclosure of personal information in the private sector, but only in the course of commercial activities. The Act also seeks to regulate employee information, but due to jurisdictional issues, only in relation to federally regulated employment. The issue brought before this Committee was whether a consent model designed for commercial contexts can be applied to the employment milieu.

[13] http://www.privcom.gc.ca/fs-fi/02_05_d_24_e.asp.

FETCO (Federally Regulated Employers — Transportation and Communication) argued strenuously that the current consent model under PIPEDA does not lend itself to the workplace environment. A number of employment issues were raised by FETCO, some of which we have addressed elsewhere in the report (i.e. work product and business contact information). FETCO's principal concern, however, relates to consent. It is FETCO's position that a definition of "personal employee information" should be added to PIPEDA, and that employee consent should not be required for the reasonable business use, collection or disclosure of any information related to managing the employment relationship. FETCO put forth the following options in its brief to the Committee:

> Different options exist for dealing with employee consent including reliance on implied or deemed consent, or even eliminating the requirement for employee consent for the collection, use or disclosure of personal information related to managing reasonable aspects of the employment relationship (similar to the approaches used in BC and Alberta). It is recommended that issues surrounding employee consent be reconsidered and addressed during the review process (December 2006, p. 4).

Once again, reference is made to the British Columbia and Alberta *Personal Information Protection Acts* which tackle the employment issue from another angle. The Information and Privacy Commissioner for British Columbia, David Loukidelis, outlined for the Committee the approach taken in his province:

> It is not necessary for an organization in British Columbia to get employee consent to collect, use, or disclose what is called employee personal information. This is not to say that employers have free rein, however, when it comes to collecting or using their employee's personal information, because the definition of "employee personal information" stipulates very clearly that it is only the information that an employer collects solely for purposes reasonably required to establish, manage, or terminate an employment relationship with that particular individual. The legislation also imposes a requirement that any collection, or use, or disclosure of that kind of information must be for purposes reasonably related to the actual work relationship. Instead of focusing on consent, recognizing that consent in the employment context is often coerced or that employees are under pressure to agree to employer practices, recognizing that it's not appropriate, for example, to ask an employer to get the consent of an employee who's suspected of defrauding the company to being put under surveillance — you're hardly going to get the suspect who's allegedly stealing from you to consent to that — instead of having to go through the consent route, it has been decided that you should be able to collect, use, or disclose personal information so long as it fits within the definition (November 29, 2006)

At the start of our hearings, the Privacy Commissioner cautioned about adopting the Alberta and B.C. approaches to employee information. Although acknowledging that personal information about employees has been a source of some of her most challenging complaints under PIPEDA, the Commissioner expressed concern that exempting large portions of employees' personal information from the consent process would take away rights that they currently have under PIPEDA. At the end of this review process, however, the Commissioner presented us with what she believes is a means by which all concerns might be addressed. She recommended that consideration be given to adopting the Alberta model, a reasonable purposes-based employee code, that also incorporates

Quebec's approach to protecting employee personal information. Thus any exemption for employee information must be accompanied by a requirement to consider employee dignity and an assessment of whether there would be an undue intrusion into an employee's personal life.

The Commissioner stressed that setting the specifics of her proposed regime would not be easy; however, she suggested that the use of section 7 of the Act, exemptions for collection, use and disclosure without consent, could contain a provision that would permit such exemptions for the purposes of establishing, managing or terminating an employment relationship. In her opinion, incorporating the concept of dignity would also enhance the Commissioner's ability to examine the full content of a complaint, in order to ensure that an employee consent exemption is not stretched too far. In this regard, she provided an example of a consent exemption stretched to incorporate such privacy intrusions as workplace surveillance.

The Committee agrees that the consent principle in PIPEDA does not fit easily into the workplace setting; however, we are mindful that creating exceptions to the consent requirement for employee/employer relationships or creating a separate employment code, is a complex undertaking. We therefore recommend that the government look to the models that currently exist in Quebec, British Columbia and Alberta in order to craft a suitable federal approach that ensures both a workable model for the functioning of employment relationships and the protection of the privacy rights of individual employees.

Recommendation 5

The Committee recommends that the Quebec, Alberta and British Columbia private sector data protection legislation be considered for the purposes of developing and incorporating into PIPEDA an amendment to address the unique context experienced by federally regulated employers and employees.

B. Investigative Bodies

PIPEDA contains two provisions that allow for the disclosure of personal information without the knowledge or consent of the individual to an investigative body. Section 7(3)(d) provides for such disclosure to be made on the initiative of an organization to an investigative body for certain purposes, and section 7(3)(h.2) permits an investigative body to release information for purposes related to the investigation of a breach of an agreement or contravention of the laws of Canada or a province. Investigative bodies are specified by regulation, and there are currently about 75 investigative bodies so designated.

Most business organizations that we heard from felt that PIPEDA should be amended to deal with problems experienced in terms of the nature and operation of investigative bodies and the designation process. In particular, it was argued that there are

many inconsistencies between the section 7 exemptions for collection, use and disclosure that frustrate the efforts of organizations in detecting and preventing fraud. The Canadian Bankers Association had this to say in its brief to the Committee:

> There are inconsistencies between the exemptions for collection, use and disclosure in the Act that can make it difficult for the banks to prevent fraud against their customers, other customers and the bank. In their efforts to prevent and investigate fraud against their customers and the banks themselves, banks frequently encounter situations where they need to be able to collect, use and disclose personal information without consent but are unable to do so due to the Act's inconsistencies among section 7(1), 7(2) and 7(3). For instance, while the Act allows an organization to collect and disclose information relating to a breach of an agreement, it does not allow for internal use of that same information in the course of the investigation to prevent further fraud against that customer, other customers or the bank. (January 2007, p. 3)

To remedy these concerns, it was suggested by some witnesses that instead of designating investigative bodies through regulation, a definition of "investigative bodies" could be added to the Act whereby bodies could self-designate according to a list of criteria. On the other hand, many organizations argued in favour of doing away completely with the "investigative body" approach under PIPEDA. They recommended that the Committee amend PIPEDA to follow the approaches taken by Alberta and British Columbia, which define the term "investigation" and allow collection, use and disclosure without consent for that purpose. The B.C. Act specifically includes fraud prevention in its definition.

The Privacy Commissioner believes that the current approach to designating investigative bodies, though cumbersome, is working adequately and does not need to be altered at this time. In her background document prepared for the Committee, the Commissioner noted that support for the current designation process is based on the transparency and oversight that stems from the regulatory process particularly as privacy impact assessments must be submitted as part of the application process. As well, the regulatory process ensures that there is a clear public listing of organizations designated as investigative bodies under the Act.[14]

The Committee supports the idea of an investigation exception to the consent principles under PIPEDA. We are concerned about the lack of consistency in section 7 of PIPEDA in this respect and in the interests of harmonization, we recommend that the approach taken by the Alberta and British Columbia private sector legislation be followed. These two second generation Acts allow for the collection, use and disclosure of personal

[14] Office of the Privacy Commissioner of Canada, Statutory Review of the PIPEDA: Background Information on the OPC's Consultation, November 27, 2006, p. 12.

information without consent for the purposes of an investigation, which is defined to include an investigation of a breach of an agreement, a contravention of a federal or provincial law or circumstances or conduct that may result in a remedy available at law.

Recommendation 6

The Committee recommends that PIPEDA be amended to replace the "investigative bodies" designation process with a definition of "investigation" similar to that found in the Alberta and British Columbia *Personal Information Protection Acts* thereby allowing for the collection, use and disclosure of personal information without consent for that purpose.

C. Business Transactions

Numerous witnesses representing business interests spoke to the Committee about the lack of a provision in PIPEDA that would allow an organization to disclose personal information to prospective purchasers or business partners without the consent of the individual affected. Businesses often need to share information (such as client lists) to evaluate whether to proceed with a transaction — perhaps a merger, acquisition or sale of business — without the cumbersome necessity of obtaining every customer's consent.

The Privacy Commissioner's PIPEDA Review Discussion Document[15] indicates that several provincial data protection laws, such as Ontario's *Personal Health Information Protection Act* (PHIPA) and the Alberta and British Columbia *Personal Information Protection Acts* (PIPAs), allow disclosures without the individual's consent for business transaction purposes, subject to stringent confidentiality agreements. A number of witnesses before this Committee argued that it would be appropriate to include a similar provision in PIPEDA, along the lines of the Alberta or British Columbia models, to facilitate commercial transactions and to protect commercial secrets in a competitive business environment.

Section 22 of Alberta's *Personal Information Protection Act* sets out a regime for the disclosure of personal information without consent in the course of a business transaction, which is defined broadly to mean a transaction consisting of, for example, the purchase, sale, lease, merger or amalgamation or any other type of acquisition or disposal of an organization. Organizations are permitted to share personal information if necessary to determine whether to proceed with the transaction, and then to carry out the transaction. Obligations are set out for the return or destruction of the information if the transaction does not go ahead.

---

15 Ibid. p. 19.

Section 20 of the British Columbia *Personal Information Protection Act* permits similar information sharing, adding a requirement that the disclosed information be used only for the purpose for which it was collected, and that those whose personal information is disclosed are informed about the disclosure and the business transaction that has taken place.

The Canadian Medical Association asked that any new provision pertaining to the sale or transfer of a business explicitly recognize the unique situation of physicians and patient information. The Association had this to say:

> Physicians are striving to deliver timely quality care to patients, often with competing and multiple demands. Physicians are therefore seeking assurances from lawmakers that any amendments to PIPEDA will take into account the potential impact on them and their patients. Therefore, we seek assurances that, one, health care is recognized as unique when it comes to the disclosure of personal information before the transfer of a business, such as one physician transferring his or her practice to another. This is already regulated at the provincial level through the appropriate licensing bodies. As a general rule, physicians must give notice to the public, whether via a newspaper ad or a notice in the office, about the change in practice. (December 13, 2006)

The Privacy Commissioner, in her final submission to the Committee, advocated an amendment to PIPEDA that would create an enhanced version of the Alberta merger or sale of business model. In terms of enhancements, the Commissioner recommends a due diligence requirement that would limit information sharing to the least amount of personally identifiable information possible. As well, after a transfer of ownership, all individuals whose information has been transferred without consent should be notified about the transfer as soon as possible. Finally, the new owner should be required to adhere to the selling organization's policies respecting privacy until all individuals have had an opportunity to choose whether they want to have a relationship with the new owner.

This Committee agrees that PIPEDA must be amended to create an exception to the consent requirement in cases of business transactions or corporate restructuring. Indeed, we note that none of our witnesses opposed such an amendment. The question, however, is what is the best approach to facilitating these transactions while at the same time protecting, to the greatest extent possible, the privacy interests in the personal information that is shared. We note that a number of our witnesses, including the Privacy Commissioner, supported the Alberta model in particular, and we therefore recommend the adoption of this approach along with the enhancements to it that were proposed by the Commissioner.

Recommendation 7

The Committee recommends that PIPEDA be amended to include a provision permitting organizations to collect, use and disclose personal information without consent, for the purposes of a business transaction. This amendment should be modeled on the Alberta *Personal Information Protection Act* in conjunction with enhancements recommended by the Privacy Commissioner of Canada.

D. Principal-Agent Relationship

The Insurance Bureau of Canada (IBC) brought a principal-agent issue to the attention of the Committee. IBC is concerned about the lack of a provision that clarifies this relationship in PIPEDA. For example, it was pointed out that in a principal-agent relationship, the consent that is granted by the principal should be able to be relied upon by the agent in carrying out certain functions. In the insurance industry, investigations and claims settlements may be outsourced to independent adjusting companies, and IBC seems concerned that this outsourcing could be considered disclosures for the purposes of the Act and as such, would require a separate consent for the agent. In its brief to the Committee, IBC had this to say:

> Outsourcing of business functions to agents is a necessary and integral part of business practices for all business sectors. A reasonable person, who is referred to sections 3 and 5(3) of PIPEDA, would expect that an insurer, like any other business, would outsource certain functions to others who act as agents on behalf of the insurer. If the agent wants to use the personal information for its own purpose, then the agent would have to obtain a separate consent from the individual for that separate purpose. (November 24, 2006, p. 12)

IBC referred to section 12(2) of the British Columbia *Personal Information Protection Act* as a possible solution to the problem it identified. In the alternative, it suggested that definitions of “agent,” “use” and “disclose” could be added to PIPEDA. Section 12(2) of the B.C. Act provides:

> 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

The Canadian Bar Association, in its submission to the government in preparation for this review,[16] also raised the need to clarify the existence of an agent concept in PIPEDA. The Association pointed out that the third party processing rule in Principle 4.1.3 of Schedule 1 of the Act, which requires organizations to use contractual or other means to ensure a comparable level of protection while the information is being processed by a third party, does not explicitly state whether such processing is considered a transfer or a disclosure, the latter of which would require consent. As well, the Association felt that the Act is unclear about whether the processing exception is to be strictly limited to transfers of information for payroll, pensions and other such administrative purposes (i.e. as opposed, for example, to work conducted by a private investigator retained by the organization). The Association therefore suggested that PIPEDA be amended 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 individual relates, but only if the individual previously consented to the collection, use and disclosure of the information by the principal organization, and the information is collected, used and disclosed to assist in carrying out work on behalf of the principal organization.

The Committee agrees that any confusion about the existence of a principal-agent relationship in PIPEDA should be cleared up. Given that the recommendation of the Canadian Bar Association appears to be essentially the same as section 12(2) of the B.C. Act, we recommend that PIPEDA be amended to clarify the principal-agent relationship under PIPEDA with reference to the B.C. legislation.

Recommendation 8

The Committee recommends that an amendment to PIPEDA be considered to address the issue of principal-agent relationships. Reference to section 12(2) of the British Columbia *Personal Information Protection Act* should be made with respect to such an amendment.

[16] Canadian Bar Association, National Privacy and Access Law Section, Preparing for the 2006 Review of the *Personal Information Protection and Electronic Documents Act,* August 2005, pp. 21-24.

E. Litigation Process/Legal Proceedings

Related to concerns expressed by witnesses about the way in which PIPEDA applies to law enforcement/investigations (see Investigative Bodies, above), the Committee heard testimony that PIPEDA should also be rendered neutral with respect to the litigation process. Brian Bowman of the Canadian Bar Association had this to say in his submission to the Committee:

> In other words, it [PIPEDA] should not affect pre-existing and commonly held litigation processes that have evolved for decades and hundreds of years. PIPEDA contains a number of specific exemptions to the consent requirement that require amendment. 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. This narrowness is evident in the investigation exceptions, the one-way disclosure, the collection and use of debt disclosure information, and the limitation on disclosure throughout the litigation process. The result is inadequate coverage of all aspects of the process: pleadings, oral discovery, mediation, private arbitration, settlements, solicitor communications, and other non-court ordered exchanges of information. 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. (December 11, 2006)

The Canadian Bar Association recommended that the models for litigation provided in the British Columbia and Alberta *Personal Information Protection Acts* be considered in relation to PIPEDA. Sections 12, 15 and 18 of the British Columbia Act permit the collection, use and disclosure of personal information without consent where it is reasonable to expect that the collection, use or disclosure with consent would compromise the availability or accuracy of the personal information, and the collection, use or disclosure is reasonable for an investigation or proceeding. Sections 14, 17 and 20 of the Alberta Act permit the collection, use and disclosure of personal information without consent where the collection, use or disclosure is reasonable for the purposes of an investigation or a legal proceeding. Both Acts define “proceeding” and “legal proceeding” as a civil, criminal or administrative proceeding that is related to a breach of an agreement, a contravention of a federal or provincial Act or a remedy available at law or under common law or in equity.

In a somewhat similar line of argument, the Insurance Bureau of Canada (IBC) sought an exemption to the consent requirement in PIPEDA in relation to witness statements. IBC recommended that the definition of “personal information” be modified to clarify that personal information expressed by one individual (the witness) about another (the subject) is the personal information of the witness. It also felt that section 7 of PIPEDA, exemptions to the consent requirement, should be amended to provide that an organization may, during the course of investigating and settling contractual issues or claims for loss or damages, collect, use and disclose a witness statement without the subject’s knowledge or consent. The following rationale was provided for IBC’s proposals:

> In our view, it would be unreasonable to prevent the insurer — and the court and jury, if a lawsuit is commenced and the matter proceeds to trial — from collecting all of the relevant facts related to the incident. We are opposed to the view that an insurer should obtain the consent of the claimant or potential claimant before obtaining witness

> statements. This would have serious consequences as it would effectively allow one individual to prevent another individual (witness) from reporting what they saw or heard and would prevent an insurer, and by extension the court, from collecting all of the relevant facts about the incident. (November 24, 2006, brief, p. 4)

The Committee agrees that there appear to be some inconsistencies in the current exceptions to the consent provisions of PIPEDA which could be better dealt with in a broader approach. We heard testimony about this in a number of areas. Specifically, with respect to litigation or legal proceedings, the Committee believes that PIPEDA's privacy protection provisions should not impede the proper conduct of litigation, and that a broad amendment may be required to exempt from the consent requirement information necessary for legal proceedings. This should be done in a manner that would bring PIPEDA into alignment with the British Columbia and Alberta statutes.

The Committee is also concerned about the testimony it received with respect to witness statements and the issue of whose personal information is contained therein. We appreciate that insurance companies are struggling, in the course of investigating and settling insurance claims, with issues of whether, in order to obtain a witness statement, they must seek the consent of the claimant or potential claimant because his or her personal information is contained therein. As well, we received testimony that insurers are reluctant to provide access to witness statements to claimants who assert that they are entitled to these documents on the basis that it is their personal information.

While we have not heard evidence in this regard from organizations representing privacy interests, including the Federal Privacy Commissioner, we feel that consideration should be given to whether there might be ways in which the issue of witness statements could be addressed in PIPEDA other than by means of our proposed investigation exception (Recommendation 6) and the following litigation/legal proceedings exception.

Recommendation 9

The Committee recommends that PIPEDA be amended to create an exception to the consent requirement for information legally available to a party to a legal proceeding, in a manner similar to the provisions of the Alberta and British Columbia *Personal Information Protection Acts*.

Recommendation 10

The Committee recommends that the government consult with the Privacy Commissioner of Canada with respect to determining whether there is a need for further amendments to PIPEDA to address the issue of witness statements and the rights of persons whose personal information is contained therein.

F. Individual, Family and Public Interest Exceptions

Section 7(3)(e) of PIPEDA allows for a disclosure of personal information without consent "to a person who needs the information because of an emergency that threatens the life, health or security of an individual and, if the individual whom the information is about is alive, the organization informs that individual in writing without delay of the disclosure." Some witnesses, however, felt that this provision was not broad enough to cover other situations that would equally warrant such an exemption.

The Committee heard from the Insurance Bureau of Canada (IBC) and the Financial Advisors Association of Canada (Advocis) that it would be helpful to have an exemption to PIPEDA's consent requirements with respect to beneficiaries (e.g. under a will or insurance policy). IBC, for example, referred to instances within the insurance industry where a policy is applied for and issued in the name of one individual, but other individuals are named or listed as additional insureds or beneficiaries. IBC therefore asked for a provision within PIPEDA that would allow an individual to give consent on behalf of another individual when the other individual can claim the benefit of a product or service for which their personal information was provided. Reference was made to section 8(2) of the B.C. *Personal Information Protection Act* which provides that:

> 8(2) An individual is deemed to consent to the collection, use or disclosure of personal information for the purpose of his or her enrollment or coverage under an insurance, pension, benefit or similar plan, policy or contract if he or she
>
> (a) is a beneficiary or has an interest as an insured under the plan, policy or contract, and
>
> (b) is not the applicant for the plan, policy or contract.

Advocis recommended that consideration be given to section 14(a) of Alberta's *Personal Information Protection Act* for the purposes of allowing financial advisors to collect information about third parties in the course of developing a financial plan for clients. Section 14(a) allows an organization to collect personal information without consent where "a reasonable person would consider that the collection of the information is clearly in the interests of the individual and consent of the individual cannot be obtained in a timely way or the individual would not reasonably be expected to withhold consent."

The Canadian Bankers Association (CBA) raised the issues of natural disasters where family members want to determine whether a loved one has survived and are seeking information about them, and employment situations where an employer cannot reach an employee and therefore needs to convey important information to a next of kin or designated contact. The banks were also concerned about the incidence of elder financial abuse and the inability of PIPEDA to address this problem. Mr. Warren Law of the CBA outlined the banks' concern:

> An example of such a situation in the banking context is where a banker suspects financial abuse, particularly with seniors, and when a customer is withdrawing money from his or her account and it appears that the customer may be under pressure from the person accompanying him or her, or the withdrawal is uncharacteristic of that person.
>
> Prior to PIPEDA, under common law, banks were able to disclose their suspicions about abuse to the authorities, to the vulnerable customer's family, or to another responsible person who might be able to investigate and stop any abuse. Financial abuse of the elderly is a significant issue in Canada. The public and families of such customers expect bankers to help prevent any abuse. Under the current legislation, though, while branch employees want to help, they are not allowed to because there are no exceptions that cover such situations. We are recommending an exemption for disclosure without consent when it is in the public interest. (January 30, 2007)

The CBA recommends that section 7(3) of PIPEDA be amended to permit disclosure of personal information to appropriate authorities, next of kin or a designated contact for the individual when the release of that information is in the individual's or the public's interest.

In its submission to Industry Canada in anticipation of this Committee's review,[17] the Canadian Bar Association recommended that certain factors should be taken into consideration when assessing the reasonableness of relying on consent obtained indirectly from an individual through another person. For example, the nature of the transaction, the sensitivity of the personal information, the nature of the relationship between the individual and the person confirming his or her consent and whether the collection, use or disclosure benefits the individual are all factors that should be set out in the legislation as assessment criteria.

It is the Privacy Commissioner's position that there may well be some very limited exceptions in this area that should be considered for the purposes of a consent exemption. Examples cited by the Commissioner included disclosures to the family of an injured, ill or deceased individual and notification in the case of an emergency in a community setting.

As noted at the beginning of this report, the Committee generally recognizes the need to harmonize PIPEDA with provincial private sector data protection laws. This is an instance where there is a need to consider the relevant provisions found in Quebec, Alberta and B.C. The Committee is cautious, however, about recommending the use of the term "public interest" in this context given its potential vagueness and the fact that we have heard a lot of testimony around the vagueness of terms or the lack of clarity in PIPEDA's current provisions. On the other hand, we are mindful that a broad term like "public interest" may be necessary to provide sufficient flexibility to such an exemption.

---

[17] Ibid., pp. 42-43.

Recommendation 11

The Committee recommends that PIPEDA be amended to add other individual, family or public interest exemptions in order to harmonize its approach with that taken by the Quebec, Alberta and British Columbia private sector data protection Acts.

G. Law Enforcement/National Security Interests

i. Section 7(3)(c.1)

Section 7(3)(c.1) of PIPEDA allows organizations to disclose personal information to government institutions without the knowledge or consent of the individual and without judicial authorization in certain specified circumstances related to law enforcement and national security. A number of witnesses raised concerns about what is meant by "government institution" in this provision and suggested that the term be clarified because disclosures to such bodies are made without the knowledge or consent of the individual.

The Canadian Bar Association, for example, recommended that PIPEDA include a definition of "government institution" to specify whether disclosure is intended to encompass municipal, provincial, territorial, federal and non-Canadian entities. The Canadian Internet Policy and Public Interest Clinic (CPPIC) felt strongly that in view of Canadians' concerns about outsourcing of information processing and the powers of foreign agencies to access such data from private businesses, the phrase "government institutions" in sections 7(3)(c.1) and (d) of PIPEDA should be limited to Canadian government institutions. This would force foreign governments' requests for data about Canadians to be routed through Canadian government entities.

Another issue raised with respect to section 7(3)(c.1) had to do with the meaning of "lawful authority." Some witnesses, such as the BC Freedom of Information and Privacy Association and BC Civil Liberties Association were of the opinion that private companies should insist on seeing a court order from a law enforcement or investigative agency (except in exceptional and urgent cases) before disclosing any personal information pursuant to this section. On the other hand, we heard from the Canadian Association of Chiefs of Police (CACP), the Canadian Resource Centre for Victims of Crime and the RCMP that law enforcement efforts are actually being thwarted by stringent interpretations of PIPEDA with respect to obtaining non-sensitive personal information on a voluntary basis from companies. Mr. Clayton Pecknold of the Canadian Association of Chiefs of Police explained the problem to the Committee in this way:

> In another example, a police officer may be in the early stages of a missing person investigation, in which he or she is trying to determine if in fact a crime has occurred. Perhaps we may have to solicit the assistance of a financial institution because we need to know if that person bought gas at a particular gas station or if the person used a credit

> card, or perhaps we need to find out if a person has a cell phone registered to him with a particular company. For this information we rely on paragraph 7(3)(c.1), which permits disclosure upon lawful authority, as my friend has already noticed. However, we are increasingly seeing some companies interpreting lawful authority to mean that a warrant or court order is required before they comply. This is an interpretation that is not, in our respectful view, consistent with the intent of the drafting of the act. Such an interpretation by companies, while no doubt grounded in a legitimate desire to protect their customers' privacy, is overly restrictive and defeats, in our view, the intent of paragraph 7(3)(c.1).(February 13, 2007)

The CACP, the Canadian Resource Centre for Victims of Crime and the RCMP all recommended that section 7(3)(c.1) be amended to make it clear that lawful authority does not mean that a warrant is required in order for there to be a disclosure.

The Committee agrees that there is a valid concern around what constitutes lawful authority for the purposes of disclosure under section 7(3)(c.1). Clearly something other than judicial authorization is required for the purposes of this section given that section 7(3)(c) provides for disclosure without knowledge or consent in compliance with a warrant or subpoena. We think it is important, for both organizations and law enforcement agencies, that what is meant by "lawful authority" be clarified in section 7(3)(c.1). Moreover, the Committee feels that consideration should be given to changing the word "may" in the opening part of section 7(3) in order to make the provision mandatory as opposed to permissive. We appreciate that, in light of the permissive nature of section 7(3) and its fit within the general framework of the Act, this might require restricting a mandatory approach to those disclosure provisions dealing with issues of law enforcement and national security.

The Committee also agrees that there is a need to clarify what is meant by the term "government institution" in sections 7(3)(c.1) and (d) of PIPEDA. Specifically, organizations should know whether the term is intended to encompass municipal, provincial, territorial, federal and non-Canadian entities.

Recommendation 12

The Committee recommends that consideration be given to clarifying what is meant by "lawful authority" in section 7(3)(c.1) of PIPEDA and that the opening paragraph of section 7(3) be amended to read as follows: "For the purpose of clause 4.3 of Schedule 1, and despite the note that accompanies that clause, an organization shall disclose personal information without the knowledge or consent of the individual but only if the disclosure is […]"

Recommendation 13

The Committee recommends that the term "government institution" in sections 7(3)(c.1) and (d) be clarified in PIPEDA to specify whether it is intended to encompass municipal, provincial, territorial, federal and non-Canadian entities.

ii. Section 7(1)(e)

Section 7(1)(e) was added to PIPEDA pursuant to the *Public Safety Act, 2002,* which in 2004 amended a number of federal laws in response to the events of September 11, 2001 in the United States. Prior to 2004, organizations subject to PIPEDA already had the ability to *disclose* personal information without the individual's knowledge or consent for reasons of national security, the defence of Canada, the conduct of international affairs or where required by law (sections 7(3)(c.1), 7(3)(d)(ii) and 7(3)(i)). The amendments brought about by the *Public Safety Act* added the ability of organizations to *collect* and *use* personal information without knowledge or consent of the individual for the purposes of making such disclosures. It is the new collection power that is most troubling to privacy advocates.

The Committee heard from some individuals as well as privacy rights organizations who argued that section 7(1)(e) of PIPEDA not only fails to fit into the balanced consent regime under the Act, but it also blurs the line between the private sector and law enforcement.[18] Murray Long, a privacy consultant, had this to say about the section:

> To understand the impacts of this change, it is important to consider the meaning of the word "collect". Whereas "use" relates to the management and various uses of existing personal information that has previously been collected, "collect" refers to the acquiring of new information that did not previously exist within the organization.
>
> Under the *Public Safety Act* amendment, organizations can now collect new information about their customers or employees or any other party where they believe there is a national security interest and for the purpose of eventually disclosing it to a security agency.
>
> This invites tremendous abuse of individual privacy rights. (February 6, 2007, brief, p. 8)

The Privacy Commissioner, in her submission to the Committee, raised serious concerns about the broad wording of section 7(1)(e). In her view, because the provision applies to any organization subject to PIPEDA, it has the undesirable effect of deputizing

[18] Professor Colin Bennett, Submission to a House of Commons Standing Committee on Access to Information, Privacy and Ethics, November 22, 2006, p. 12.

the private sector to carry out law enforcement activities without the corresponding public accountability.[19] As she did at the time of the passage of the *Public Safety Act, 2002,* the Commissioner continues to call for the removal of section 7(1)(e) from PIPEDA, or that it at least be made more restrictive.

In a letter dated March 20, 2007, that was hand delivered by the Chairman on that same day, the Committee asked the Minister of Public Safety for his assistance in addressing the issues raised by our witnesses on this matter. Specifically, the Minister was asked to appear or provide written comments within a week or so in order that the Committee could be timely in its reporting to the House of Commons. In the absence of any such response from the Minister, based on the testimony it received, and after considered debate by Committee Members, the Committee makes the following recommendation.

Recommendation 14

The Committee recommends the removal of section 7(1)(e) from PIPEDA.

PERSONAL INFORMATION OF MINORS

Some witnesses advocated including in PIPEDA special rules designed to protect children from improper collection, use or disclosure of their personal information. Professor Valerie Steeves, of the University of Ottawa, impressed upon the Committee the subtle ways in which children's personal information is collected when they are on the Internet. She described popular websites where, in order to be allowed to play the games available there, children must first fill out marketing surveys.

> These kids are nine and they are playing. They are not disclosing information for commercial purposes. Yet the kind of legislation that we have in place lets companies set up these kinds of environments and, through a very weak consent mechanism, capture that information and reconfigure it as a commercial commodity. (November 29, 2006)

Philippa Lawson, of the Canadian Internet Policy and Public Interest Clinic (CIPPIC), urged the Committee to recommend amendments to PIPEDA to create "special limitations regarding the collection of information from children, whose credulity and ignorance can easily be exploited by commercial interests."[20] CIPPIC recommended that there be included in the Act specific rules limiting the collection, use and disclosure of

---

19 Footnote 14, p. 11.

20 December 6, 2006.

children's personal information, along with strict penalties for violating these provisions. Reference was made in this respect to the *Canadian Code of Practice for Consumer Protection in Electronic Commerce* by the Canadian Marketing Association.

Responding to a discussion about the collection of personal information from children, the Information and Privacy Commissioner for British Columbia, David Loukidelis, made the following comments, saying that while some legislative steps have been taken in the United States, the issue is still under consideration in Canada.

> On the question of surveying children, clearly that introduces some very sensitive issues around the ability of youth to understand what it is they're entering into when they give up some of this information, sufficiently so that in the U.S., Congress passed the Children's Online Privacy Protection Act of 1998. Again, it is early days for these laws in Canada. For my part, I would hope that in British Columbia, we can, only three years into our law, continue to work with industry to try to ensure that in the case of children and generally in relation to some of these technological challenges, those general principles are adhered to and that the legislation works well in its present form without radically altering the approach to some of these technologies. (November 29, 2006)

The Canadian Bar Association (CBA) included a short discussion of issues relating to consent by minors in the brief it prepared in anticipation of the 2006 PIPEDA Review.[21] The CBA argued that there is uncertainty about whether minors can consent to participate in on-line activities without parental consent. Clarification is called for, it contends, about when minors can give such consent, and consideration should be given to stipulating a minimum age below which consent may not be given without parental approval. The CBA recommended that PIPEDA be amended to provide that minors can consent to the collection, use and disclosure of their personal information if they understand the nature of giving consent and its consequences, and that below a certain age (for example, 13 years) such consent must be given by a parent or legal guardian.

While the Privacy Commissioner's background document, *Statutory Review of the PIPEDA: Background Information on the OPC's Consultation,*[22] mentions that the issue of the personal information of minors was brought forward in its consultations by a consumer advocacy group, the Commissioner herself did not take a position on whether the Act should be amended to deal with it. This may be because the establishment of a specific age at which children are competent to act independently is an area of provincial jurisdiction. Nonetheless, the Committee believes that the issue of consent with respect to the collection, use and disclosure of personal information of minors in a commercial context is of sufficient importance to merit further study, including input from the Privacy Commissioner and other stakeholders.

---

21 See footnote 16, pp. 43-44.

22 See footnote 14, p. 33.

Recommendation 15

The Committee recommends that the government examine the issue of consent by minors with respect to the collection, use and disclosure of their personal information in a commercial context with a view to amendments to PIPEDA in this regard.

DATA OUTSOURCING (TRANSBORDER FLOWS OF PERSONAL INFORMATION)

In today's high-tech, globalized business environment, more and more information is being outsourced for processing. Along with this growing practice, however, comes the question of the extent to which Canadian privacy protection at home travels with personal information that is transferred to non-Canadian organizations. Most businesses feel that PIPEDA currently offers adequate privacy protection in this respect. Reference is made to PIPEDA's Accountability Principle (Principle 1, Schedule 1) which states that each organization is responsible for the personal information in its care. Specifically, Principle 4.1.3. provides that this responsibility extends to information that has been transferred to a third party for processing. The Information Technology Association of Canada (ITAC), in its brief to the Committee, summed up the views of the business community this way:

> PIPEDA's accountability principle demands that businesses in Canada communicate their privacy practices to the public in a transparent manner. It also requires that those businesses enter into contractual agreements with their third-party providers in all jurisdictions to ensure a similar level of protection for personal information transferred outside Canada. In this respect, PIPEDA, together with the law of contract and agency, works to deal with practical business, legal and technological realities […] Placing further restrictions on transborder flows of information under PIPEDA could reduce the competitiveness of Canadian businesses in the global market. (December 11, 2006, p. 4)

Other witnesses, however, sought greater privacy protection mechanisms for trans-border information-sharing by the private sector. Arguments were made for more specific rules directed at the protection of personal information transferred outside of Canada and reference was made to the Quebec *An Act Respecting the Protection of Personal Information in the Private Sector*[23] which obliges people communicating information about Quebec residents to persons outside the province to take all reasonable care to ensure that the information is not disclosed to third parties without consent, except as provided by legislation. In his submission to the Committee, Brian Bowman of the Canadian Bar Association made a number of suggestions for consideration in this area:

[23] Section 17.

> PIPEDA should contain appropriate precautionary requirements to protect information when it is transferred across borders. We have previously considered a number of alternatives to achieve this objective, such as a requirement that organizations transferring information to foreign entities enter into written agreements that would ensure security and protection of information against unauthorized access or disclosure in accordance with Canadian privacy law […] In its earlier submission, the CBA section also analyzed options for notification or consent requirement for information transferred across a border. Each of these options would involve some form of notice to be provided to or consent obtained from the individuals whose information would be transferred outside of Canada. Amending PIPEDA to implement either a notice or a consent requirement to cross-border transfer of information requires a very careful consideration of the potential advantages and disadvantages of the approach. (December 11, 2006)

The B.C. Freedom of Information and Privacy Association and BC Civil Liberties Association also reminded us of the situation that arose in British Columbia with respect to the outsourcing of medical records to the United States and concerns about the reach of the U.S. *Patriot Act.* That law was passed in the wake of the events of September 11, 2001 as a means of increasing the U.S. government's ability to conduct searches and to seize or compel the disclosure of records. The B.C. government ultimately amended its public sector privacy legislation to address the concerns about possible unauthorized disclosures of personal information to U.S. authorities. In his appearance before the Committee, the Information and Privacy Commissioner for British Columbia, David Loukidelis, spoke to the B.C. outsourcing issue and outlined what he sees as the distinction between public and private sector data protection legislation in relation to trans-border information flows:

> The legislature, three weeks before that report was actually delivered with that conclusion, chose to amend the Freedom of Information and Protection of Privacy Act to make it even clearer that foreign court orders, foreign judicial process, could not reach extraterritorially into Canada with that effect, and to impose certain other requirements on public bodies in British Columbia around the protection of personal information of citizens.
>
> No such amendments were made to the *Personal Information Protection Act*. And I have from the outset, as it happens, drawn a distinction between the public sector situation, where citizens are not in a position to consent or not to consent to the decision by government to outsource the delivery of public services involving their personal health information, and the situation in the private sector, where, certainly in principle and I think realistically in practice, individuals can vote with their feet. If they're not content with the personal information practices of a particular business, they can take their business elsewhere and make that consumer choice. I think that is a real and meaningful and substantial distinction that justifies the different treatment across the public sector and private sector divide. (November 29, 2006)

The Federal Privacy Commissioner also sees no need for amendments to the federal private sector data protection legislation to deal with data outsourcing. In her view, this matter is best addressed through the guidance of PIPEDA's Accountability Principle

along with existing Treasury Board guidelines on contracting out.[24] The Commissioner pointed out that she is also working on this issue at the international level. For example, she is chairing a Working Group of the Organization for Economic Co-operation and Development (OECD) Working Party on Information Security and Privacy to address the cross-border challenges of effectively enforcing privacy laws.

The Committee agrees with the Privacy Commissioner that there is no need to amend PIPEDA with respect to transborder flows of personal information. In our view, the Act already contains sufficient accountability and allows for the necessary flexibility for businesses to ensure that personal information is privacy protected when it crosses our borders. We do, however, encourage the Commissioner to continue to work with organizations, as well as the federal government, to ensure appropriate guidance in this respect.

Recommendation 16

The Committee recommends that no amendments be made to PIPEDA with respect to transborder flows of personal information.

PERSONAL HEALTH INFORMATION

Although PIPEDA came into force on January 1, 2001, as a result of Senate amendments to Bill C-6 (PIPEDA), the law did not apply to personal health information until January 1, 2002. In its December 1999 report, the Standing Senate Committee on Social Affairs, Science and Technology observed a considerable amount of uncertainty surrounding the application of the privacy protection provisions of Bill C-6 to personal health information.

The Senate Committee felt that this uncertainty required clarification and that further legislative action was desirable. In particular, it was felt that more specific provisions regarding, for example, issues of informed consent and the secondary use of personal health information should be developed. The Committee therefore recommended that the bill be amended to include a definition of “personal health information”, and that the application of the law to personal health information be suspended for a period of one year following the coming into force of the bill. The Committee hoped that this temporary suspension of Part 1 of the bill would motivate stakeholders and governments to formulate an appropriate solution for the protection of personal health information.

[24] “Privacy Matters: The Federal Strategy to Address concerns About the USA Patriot Act and Transborder Data Flows.” Treasury Board of Canada Secretariat, http://www.tbs.sct.gc.ca/pubs_pol/gospubs/TBM_128/pm-prp/pm-prp_e.asp.

According to testimony that this Committee received during its review of PIPEDA, the delayed application of PIPEDA to personal health information allowed the federal government to work with the health care community, in conjunction with the Office of the Privacy Commissioner, on the development of a set of guidelines known as PIPEDA Awareness Raising Tools (PARTs). Dr. Wayne Halstrom, of the Canadian Dental Association (CDA), had this to say about the PARTs initiative:

> We at the CDA appreciated the federal government's initiative to produce information that would help our members understand their obligations under PIPEDA versus simply obtaining another legal opinion on how PIPEDA would apply to dentists. CDA was an integral member of the working group that met regularly with officials from the Privacy Commissioner's office, Justice Canada, Health Canada and Industry Canada to create the PIPEDA awareness-raising tools, as we've heard, the PARTs initiative for the health sector. This process created the final content for the federal government's interpretation of PIPEDA, a series of straightforward questions and answers that add clarity to the requirements around obtaining consent, disclosing personal health information to private insurance companies, office safeguards, and requests to change information on a dental record, to name but a few. (December 13, 2006)

While the CDA, the Canadian Medical Association and the Canadian Pharmacists Association all expressed support for the PARTs initiative, they also recommended that the PARTs document be given legal status or, in some way, referenced within PIPEDA. The Canadian Health Infoway Inc., in its brief to the Committee, also felt that this review would be an opportune time to clarify PIPEDA's application to the health care sector.[25]

The Committee appreciates the desire for clarity and consistency in terms of the application of PIPEDA to personal health information; however, we are not comfortable with adding yet another schedule to the Act, particularly when the PARTs document is essentially a question and answer sheet that is intended to assist in the understanding of PIPEDA and not serve as legal advice. The Committee therefore recommends that the government consult further with health care stakeholders, as well as the Office of the Privacy Commissioner in order to ascertain what, if anything, can be done to reference the elements set out in PARTs (e.g. with respect to implied consent) within the legislative framework of PIPEDA.

Recommendation 17

The Committee recommends that the government consult with members of the health care sector, as well as the Privacy Commissioner of Canada, to determine the extent to which elements contained in the PIPEDA Awareness Raising Tools document may be set out in legislative form.

[25] February 2007.

POWERS OF THE FEDERAL PRIVACY COMMISSIONER

1. Order-making Powers

As noted at the beginning of this report,[26] PIPEDA is based on an ombudsman model in that the primary duty of the Privacy Commissioner is to investigate and make recommendations with respect to complaints from persons alleging that their privacy rights have been breached under the Act. The Supreme Court of Canada in *Lavigne* v. *Canada (Office of the Commissioner of Official Languages)*[27], describes the ombudsman role as follows:

> An ombudsman is not counsel for the complainant. His or her duty is to examine both sides of the dispute, assess the harm that has been done and recommend ways of remedying it. The ombudsman's preferred methods are discussion and settlement by mutual agreement.

Thus, while the Privacy Commissioner has investigative powers, the discretion to initiate complaints, the power to conduct an audit and publicly disclose information relating to the personal information management practices of an organization, she has no order-making powers under the Act.

A number of witnesses who appeared before us wanted PIPEDA amended to provide the Commissioner with order-making powers. It was argued that such powers would serve as a means of facilitating compliance with PIPEDA, cut costs and delays in the current process and generate a consistent body of case law that would allow both individuals and organizations to have a clearer understanding of their rights and responsibilities. Professor Colin Bennett, of the University of Victoria, expressed concern that the ombudsman model might not be the best fit with a private sector compliance law:

> The lesson I draw from this is that the ombudsman model, which is very good at mediating and resolving disputes between individuals and organizations, may not be very good when you're looking at a compliance model or regulatory model like this, where you're simply trying to get the organization concerned to comply with the law. Therefore, I think there's a mismatch between some of the goals of the law and the ombudsman model that is used to enforce it. (November 22, 2006)

Those favouring order-making powers for the Privacy Commissioner also referred to the three provinces with substantially similar private sector privacy legislation (Quebec, Alberta and British Columbia) wherein each privacy commissioner has the power to render binding decisions in certain cases. Referred to as "ombudsmen with a stick," these

---

[26] Overview of the Act.

[27] *Lavigne v. Canada (Office of the Commissioner of Official Languages)*, [2002] 2 S.C.R. 773, at paragraph 39.

commissioners use their order powers sparingly; however, it is argued that the strong incentive these powers provide in facilitating reasonable settlements is essential to their overall effectiveness as commissioners.

In his appearance before the Committee, David Loukidelis, Information and Privacy Commissioner for British Columbia, had this to say about his order-making powers:

> Since the beginning of 2004, we've had an order-making power. However, it has to be emphasized that it is by no means the tool of first choice for our office, speaking for myself or indeed looking at the experience of our office […] In the three years, just about, that PIPA has been in force, I've issued seven binding orders under PIPA. The remainder of the matters we have been able to deal with in a mediation type of approach, which is consistent with the approach taken, as I understand it, in every important respect, here in Ottawa by my federal colleague and in other commissioners' offices across the country. (November 29, 2006)

Most businesses and organizations who spoke to this issue preferred to maintain the existing ombudsman model because it provides a flexible, informal, accessible and cost-effective dispute resolution process with formal and binding review still available via the courts. Put another way, they feel that the current model effectively balances the rights of individuals to the protection of their personal information and the rights of organizations to use that information in legitimate ways for their commercial purposes. Organizations prefer to work with the Privacy Commissioner on a collaborative basis to help them better understand what is and is not required in order to achieve reasonable and appropriate privacy protection. A focus on working with parties to resolve issues is seen as more productive than a complaint-based approach that is adversarial in nature and directed only towards enforcing a charge of a breach of the Act.

John Gustavson of the Canadian Marketing Association had this to say about the benefits of the ombudsman model:

> The evidence of the past few years clearly indicates that the ombudsman model has worked very well in promoting and protecting the privacy rights of Canadians. In response to complaints, organizations have invariably demonstrated a willingness to follow the direction of the Privacy Commissioner. We also feel that the commissioner's role as a privacy advocate is one that inherently contains positional bias and is therefore more compatible with an ombudsman's role. Most importantly, however, the reality is that the commissioner's powers of influence are well supported by the discretionary power to publicize privacy breaches and by the ability to seek binding orders through the Federal Court. (December 4, 2006)

For her part, the Federal Privacy Commissioner made it clear that she was not seeking any changes to her powers at this time.

> In our view, now is not the best time to move on the order-making power issue. The Office of the Privacy Commissioner has tried to do its job over the last three-and-a-half years in an atmosphere of instability, constant and detailed scrutiny and reduced administrative capacity. We are just emerging from this period, renewed, rehabilitated

> and having received sufficient resources. In our view, the administrative consequences of introducing an order-making power at this time would reduce the efficiency of the OPC in carrying out its multi-faceted mandate (November 27, 2006, brief, p. 6)

Moreover, the Commissioner has indicated that the Act has not been in force long enough for her to utilize all the powers of enforcement available to her. For example, she has yet to explore the potential to seek damage awards before the Federal Court, the extent of her auditing powers has yet to be tested, and there are penal provisions under the Act that have not yet been used.

In view of the concerns raised by the Federal Privacy Commissioner, this Committee believes that now is not the time to make changes to the Commissioner's enforcement powers under the Act. We feel that there is merit in the ombudsman approach in terms of ensuring the compliance of organizations that are subject to privacy complaints. Moreover, we agree that it would be premature to consider adding order-making to the Commissioner's enforcement powers before she has had a chance to more fully explore and make greater use of all her existing powers under the law.

The Committee acknowledges that there may come a time in the future when it may be necessary to recommend such order-making powers be granted to the Commissioner if further experience demonstrates that the Commissioner's existing powers prove insufficient to properly administer respect for, and compliance with, the Act. The Committee is also mindful of the fact that any consideration of changes to the powers of the Privacy Commissioner must be studied carefully in the context of the interrelationship between her office and that of the Information Commissioner of Canada, and we flag this point for any future study of this issue.

Recommendation 18

The Committee recommends that the Federal Privacy Commissioner not be granted order-making powers at this time.

2. Naming Names

Currently, section 20(1) of PIPEDA obliges confidentiality on the part of the Commissioner, or any person acting on her behalf or under her direction, with respect to information that comes to their knowledge as a result of the performance of their duties under the Act. Subsection 20(2), however, allows the Commissioner to make public any information relating to the personal information management practices of an organization, if the Commissioner considers that it is in the public interest to do so. It is this limited exemption that was the focus of testimony by witnesses before this Committee.

Many privacy advocates called upon the Committee to amend PIPEDA to require the Commissioner to publicly name all organizations that have been found to have violated the Act. It was argued, for example, that organizations should be held publicly accountable for their actions and that if there are no order-making powers to ensure compliance, then the public should be able to hold violators accountable. Philippa Lawson, of the Canadian Internet Policy and Public Interest Clinic (CIPPIC), made her argument in the following terms:

> The Office of the Privacy Commissioner is being far too reluctant to use the powers of her office that she does have. Chief amongst these is the power to make any information gathered in her inquiries under the act public, if it is in the public interest. And this is subsection 20(2). The Commissioner has effectively indicated that she will never use it. Maybe, just maybe, she will for repeat offenders. [...] However, if consumers are to have any effect on the bad actors in the industry on the subject of privacy, they must be able to express their displeasure to the company involved. This cannot be done when the company is protected from any adverse publicity or consumer action. If this committee does not recommend full order-making power for the commission, then at the least we are calling for you to ask that the present section 20 of PIPEDA be reviewed and amended to direct the publication of names of respondents. (December 6, 2006)

Organizations, on the other hand, felt that the Commissioner's power in this respect should remain discretionary. The naming of every organization in every instance where there has been a finding of non-compliance by the Commissioner could be injurious to a business' reputation and, in fact, mislead consumers (i.e. in instances of a minor error that has been corrected with no harm to the consumer or where the issue involves only one arm of a large corporation). Ariane Siegel, for the Information Technology Association of Canada (ITAC), argued:

> Currently, case summaries are reported for the most part on an anonymous basis. The Commissioner has taken the position that naming respondents in each and every case would not meet the public interest threshold of the legislation. ITAC supports this approach. The Commissioner has the discretion she requires in order to name respondents. ITAC believes that a mandatory practice of naming respondents in each and every instance would not benefit parties to any dispute, and, in fact, could result in negative consequences. Complaint resolution often results in a change to business policies or procedures such that the benefit naturally accrues to all customers. In this way, positive results are achieved with a high degree of efficiency. (December 11, 2006)

Although the Commissioner did not provide the Committee with detailed recommendations on this matter, she did provide an article she wrote that outlines her position on naming organizations under PIPEDA.[28] The Commissioner stresses the obligation of confidentiality as being integral to the ombudsman approach in that it enables complainants to be more forthcoming, open and vulnerable, while at the same time allowing respondents to be self-critical and willing to espouse a change of practice. That

[28] Jennifer Stoddart, "Cherry Picking Among Apples and Oranges: Refocusing Current Debate About the Merits of the Ombuds-Model under PIPEDA", *Canadian Business Law Journal*, Volume 44, No. 1 pp. 9-12.

being said, she acknowledges that the Act does provide for an exception to the confidentiality rule where it is in the public interest. Given that this is a limited exception, she sets out a number of criteria that should apply to its application. For example, decisions to disclose should be on a case by case basis, there must be some reason for the disclosure which is rationally connected to the purpose for which the discretion is granted, and the extent of the disclosure should be limited to that information necessary to meet the specified purpose.

For many of the same reasons given with respect to the issue of order-making powers, this Committee feels that now is not the time to alter the naming power of the Commissioner. The Committee supports the Commissioner's approach to the use of her discretionary powers under section 20(2), and recommends that no changes be made to the Act in this regard.

Recommendation 19

The Committee recommends that no amendment be made to section 20(2) of PIPEDA with respect to the Privacy Commissioner's discretionary power to publicly name organizations in the public interest.

3. Sharing Information with other Data Authorities

As noted with respect to the issue of naming names, the Privacy Commissioner is generally required to treat as confidential any information that is obtained in the exercise of her powers. In other words, the Office is not permitted, except in certain limited circumstances, to share information about a complainant without his or her consent. Section 23 of PIPEDA does allow the Commissioner to consult with any person whose powers and duties under substantially similar provincial legislation are like those of the Commissioner. This means that the Commissioner is able to share information and cooperate in investigations of mutual interest with her counterparts in Ontario (only with respect to Ontario health information), Alberta, British Columbia and Quebec. This power does not, however, extend to cooperative efforts with respect to data protection authorities in any other provinces or jurisdictions. The Commissioner is seeking an amendment to PIPEDA to grant her this specific authority.

According to testimony provided by the Privacy Commissioner, in view of the fact that we now live in a world of increasingly virtual borders where privacy issues know no national boundaries, it is imperative that data protection authorities have the ability to work together with consumer protection and other enforcement bodies on issues of mutual concern. Apparently, many data protection authorities around the world are already looking at ways in which they can work in closer contact. By way of example, the Commissioner is currently chairing an Organization for Economic Co-operation and Development (OECD) group that is exploring ways to encourage cooperation between data protection authorities and other enforcement bodies with respect to cross-border complaints and cases arising

from transborder data flows. The U.S. Federal Trade Commission also now has the ability to share confidential information with foreign law enforcers, subject to appropriate confidentiality assurances.

The Commissioner was supported in her request by other witnesses, in particular, the Information and Privacy Commissioner for British Columbia, David Loukidelis, who felt that the Federal Commissioner should have explicit authority for cooperative investigation, enforcement and other activities with privacy commissioners and data protection authorities outside Canada, particularly in Asia-Pacific region, the United States and the European Union.[29]

The Committee agrees that in a networked global economy, privacy issues are no longer isolated incidents within provincial or national borders. At a time of increasing trans-border information sharing, protecting the personal information of Canadians may require protection mechanisms both within and outside of Canada. It would appear as well that work is already underway in terms of the creation of an international privacy protection framework as an extension of jurisdictional mechanisms. This Committee therefore recommends that consideration be given to including a provision within PIPEDA that would grant the Commissioner the authority to share personal information with her provincial counterparts that do not have substantially similar private sector legislation as well as with her international counterparts while cooperating on investigations of interest to Canadians.

In making this recommendation, the Committee is mindful of the concerns of Canadians with respect to the privacy protection of any personal information that crosses our borders. Specifically, there are concerns about the risks posed by transfers of personal information to the United States in view of the U.S. *Patriot Act*, which was passed in the wake of the events of September 11, 2001 as a means of increasing the U.S. government's ability to conduct searches and to seize or compel the disclosure of records. The Committee therefore recommends that the government also consider how information shared between data protection authorities can be adequately protected from disclosure to a foreign court or other government authority for purposes other than those for which it was shared.

Recommendation 20

The Committee recommends that the Federal Privacy Commissioner be granted the authority under PIPEDA to share personal information and cooperate in investigations of mutual interest with provincial counterparts that do not have substantially similar private sector legislation, as well as international data protection authorities.

[29] November 29, 2006, brief, p. 3.

Recommendation 21

The Committee recommends that any extra-jurisdictional information sharing, particularly to the United States, be adequately protected from disclosure to a foreign court or other government authority for purposes other than those for which it was shared.

4. Solicitor-Client Privilege

Under PIPEDA, individuals have a broad right of access to their personal information held by an organization; however, section 9 of the Act sets out a limited number of circumstances when an organization may refuse an access request. One exception to the access requirement is where the information is protected by solicitor-client privilege (section 9(3)(a) of PIPEDA). Where an organization seeks to withhold personal information on this basis, a complaint may be filed with the Privacy Commissioner who, in turn, is obliged to conduct an investigation of the matter. Pursuant to this investigation power, the Privacy Commissioner argues that she has a need to examine the documents for which solicitor-client privilege is claimed in order to determine whether they were properly withheld pursuant to the Act. It is a power that she currently has under section 34(2) of the *Privacy Act* and she testified that a similar provision was not added to PIPEDA because no one thought it would be a problem. The matter is currently before the courts.

The Privacy Commissioner specifically asked the Committee to address the impact of the recent Federal Court of Appeal decision in *Blood Tribe*[30], which could allow organizations to use any claim of solicitor-client privilege to prevent her from reviewing documents in the course of investigations. Pursuant to this decision, the Commissioner would not have the power to compel and review those documents in order to verify that they did, in fact, contain information subject to solicitor-client privilege. The Commissioner described her concern in the following words:

> I'd like to raise one very specific and I think pressing matter that relates to a recent Federal Court of Appeal decision. This case deals with solicitor-client privilege and our ability to obtain access to documents in the course of our investigations. This recent decision in the Blood Tribe case leaves a gaping hole in our ability to conduct meaningful investigations. It effectively allows organizations to shield information from our investigators with no independent verification that the documents in question do in fact contain information subject to solicitor-client privilege. Although we are seeking leave to appeal, we believe this ambiguity in the legislation needs to be clarified with an amendment to PIPEDA as soon as possible. (November 27, 2006)

[30] *Blood Tribe Department of Health v. Privacy Commissioner of Canada*, (2006) FCA 334, Fed. CA, reversing *Blood Tribe Department of Health v. Canada (Privacy Commissioner)* (2005) 40 CPR (4th) 7, Fed. Ct. (TD).

In the *Blood Tribe* case, the Federal Court of Appeal considered the power of the Commissioner to compel the production of documents in respect of which solicitor-client privilege was claimed, and found that Parliament, in enacting PIPEDA, had not intended the Commissioner's investigative powers to be unfettered by questions of solicitor-client privilege. The Court held that express statutory language would be required to abrogate solicitor-client privilege, and in the absence of such language, the Commissioner did not have the power to compel production of the documents in order to verify the claim of privilege. The Court noted that in cases where a broad claim of solicitor-client privilege is used as a shield to thwart an investigation, the Commissioner has the power to go to the Federal Court under section 15 of PIPEDA and have the claim of privilege reviewed by a Federal Court judge.

Vivian Bercovici, for the Dominion of Canada General Insurance Company, supported the decision of the Federal Court of Appeal in *Blood Tribe* and argued strongly against the amendment being sought by the Privacy Commissioner:

> [S]olicitor-client privilege goes to the heart of the order and integrity of our system of justice. An individual or party in any proceeding must know with confidence that any communication with their solicitor will not be disclosed. This allows free and unthreatened communication between solicitor and client, which facilitates the preparation and execution of a full and vigorous defence. The impact of qualifying solicitor-client privilege, which has anchored a common law tradition for centuries, would be seismic (February 6, 2007)

The Committee is in agreement with the Commissioner that there should be a means of independently verifying the appropriateness of a claim of solicitor-client privilege in respect of the denial of access to personal information under section 9 of PIPEDA. However, we disagree that the verification should stem from the Commissioner's investigative process and powers. We are also not convinced that section 15 of PIPEDA currently provides an avenue for the Commissioner to challenge a claim of solicitor-client privilege before the Federal Court in cases where she is unable to review the documents at issue. We therefore recommend that PIPEDA be amended to permit the Privacy Commissioner to apply for an expedited review of the claim of solicitor-client privilege by a judge of the Federal Court. If the judge determines that the claim of solicitor-client privilege was improperly invoked, then the Court could order that the documents at issue be produced to the individual.

The Committee recognizes that its recommendation in this context will result in an approach that is different from that taken under the *Privacy Act;* however, given that PIPEDA is different in origin and purpose from the federal public sector law, we do not feel obliged to import principles from the latter into the former.

Recommendation 22

The Committee recommends that PIPEDA be amended to permit the Privacy Commissioner to apply to the Federal Court for an expedited review of a claim of solicitor-client privilege in respect of the denial of access to personal information (section 9(3)(a)) where the Commissioner has sought, and been denied, production of the information in the course of an investigation.

BREACH NOTIFICATION

An issue addressed by most of our witnesses was the question of an organization's duty to notify individuals in instances of security breaches of personal information holdings. Currently, notification is voluntary, although the Committee was told that, in practice, organizations often consult the Office of the Privacy Commissioner in order to determine whether and, if so, how to notify their customers that a breach has occurred. Business response to security breaches can therefore vary widely, depending on factors such as the number of individuals affected, the nature of the information that was lost, and the likelihood that it could be accessed by someone who would use it for wrongful purposes. As more stories of major breaches involving the personal information of large numbers of Canadians are covered in our daily newspapers, concern about this issue is growing.

Many U.S. states have passed legislation requiring that customers be notified when their personal information has been compromised. These laws typically provide for large fines for failure to notify. In Canada, only Ontario's *Personal Health Information Protection Act* requires notification after a security breach. That Act requires health information custodians to notify individuals at the first reasonable opportunity if their personal health information is stolen, lost, or accessed by unauthorized persons.[31]

Businesses, for the most part, feel that they already have a duty to notify individuals in instances of significant security breaches involving personal information. They note that the Openness Principle (Principle 8) of the CSA Model Code, which is found in Schedule 1 of PIPEDA, suggests that organizations have responsibilities along these lines and consequently, there is no need for specific legislative provisions at this time. The Canadian Life and Health Insurance Association Inc. outlined its self-assessed, risk-based approach to notification:

> The industry supports a risk-based approach to notification, where the need to notify and the method of notifying the individual are proportional to the risk of harm that may be experienced by those whose personal information has been compromised. Under such an approach, any notification requirement would only be necessary where the breach is

[31] Section 12(21)

> material; where the organization has reasonable grounds to believe that disclosure of personal information to unauthorized individuals has taken place; and, where the disclosure presents a significant risk of harm to individuals (e.g. identity theft or fraud). (February 1, 2007, brief, pp. 11-12.)

Industry groups were generally supportive of guidance provided by the Privacy Commissioners of Canada, British Columbia and Ontario. The Ontario and British Columbia Information and Privacy Commissioners have together issued a *Breach Notification Assessment Tool*[32] to assist organizations in determining what steps should be taken in the event of a privacy breach. The Federal Commissioner and her office are also working with industry to develop voluntary guidelines to govern organizations' responses to security breaches. As the Committee was told by David Elder, of the Canadian Chamber of Commerce:

> The Canadian Chamber does not believe that mandatory breach notification is necessary in the legislation. We would encourage businesses to continue to work closely with the Privacy Commissioner's office in order to identify breaches and to notify those who could be affected by a possible breach in privacy. This flexibility enables notice where appropriate in the circumstances, with no adverse impact on consumers. I'd also like to note that it would be beneficial for the Canadian Chamber and other business associations to develop a best practices set of guidelines that could be used when breaches in privacy occur. To that end, business groups, including the Canadian Chamber, ITAC, the CMA, and others, are currently developing breach notification guidelines in conjunction with the Office of the Privacy Commissioner. Details on these best practices guidelines should be available later this spring. (February 1, 2007)

Those who argued in favour of a mandatory breach notification provision in PIPEDA spoke of the need to inform consumers in order for them to be able to effectively fight the increasing incidents of identity theft in this country. In its brief to the Committee, the Public Interest Advocacy Centre had this to say:

> The only way true accountability can be achieved is by imposing upon every organization a legal obligation to report any data leak to the OPCC and to notify all individuals whose personal information has been the subject of a security breach. Furthermore, this notification should not be qualified or diluted in any way. Every time the security of someone's personal information is breached, it should be incumbent upon the organization charged with securing and protecting that information to inform the individual of the breach. This provides every individual the autonomy to make their own decision concerning what measures to take next. It should not be up to the organization to unilaterally decide the level of risk caused by the breach or the severity of the potential harm. (October 23, 2006, p. 19)

---

[32] B.C. and Ontario Information and Privacy Commissioners, *Breach Notification Assessment Tool*, December 2006, http://www.ipc.on.ca/images/Resources/up-ipc_bc_breach.pdf.

The Canadian Internet Policy and Public Interest Clinic (CIPPIC) issued a White Paper on Breach Notification[33] that makes specific recommendations for amending PIPEDA. The paper calls for a Canadian law requiring organizations to notify individuals when their personal information has been compromised as a result of a breach of the organization's security. In particular, it calls for an amendment to PIPEDA to provide for mandatory notification of security breaches when certain types of personal information are exposed to unauthorized access as a result of a security breach. The White Paper analyzes, and in some cases adopts, certain aspects of security breach legislation in the United States, where over half the states have enacted a mandatory security breach disclosure requirement, and where several federal bills are currently pending.

Privacy expert, Murray Long, also provided the Committee with a specific four-point proposal for breach notification. First, there should be a duty to notify that would apply to all types of sensitive information, not just financial data. Second, organizations should have some discretion to determine when to notify the public, but that should be based upon their self-assessment and an objective standard, to ensure that organizations act prudently. The objective standard would require that organizations notify the Privacy Commissioner when a reasonable person would consider it appropriate to do so, and that they do so within a short, legally-prescribed timeframe. Third, when they notify the Privacy Commissioner, organizations would be required to describe the impacts of the breach, the efforts taken to mitigate it, and what decision was made to notify affected persons. If they decided not to notify persons, they would be required to explain that decision, and the Privacy Commissioner could then evaluate their decision. Fourth, it should be an offence under the Act to fail to disclose notice of a breach where a reasonable person would expect that disclosure to have taken place.[34]

The Information and Privacy Commissioner for British Columbia, David Loukidelis, cautioned against following the notification requirements adopted in some U.S. jurisdictions, arguing that there is no evidence available yet to demonstrate that mandatory notification is actually a cost-effective way to reduce the risk of identity theft related to security breaches.

In her initial appearance before the Committee, the Federal Privacy Commissioner was also cautious in her approach to this issue. While supporting the notion of a duty to notify, the Commissioner pointed to the difficulty of choosing an appropriate model and she noted that a duty to notify did not easily fit into the current PIPEDA model since there is no straightforward way to penalize organizations that fail to notify individuals about security breaches. The Commissioner did, however, recommend that in addition to adding a duty to notify, or as an alternative, a provision could be added to PIPEDA which would allow an

---

33 Canadian Internet Policy and Public Interest Clinic, *Approaches to Security Breach Notification: A White Paper*, January 9, 2007, http://www.cippic.ca/en/bulletin/BreachNotification_9jan07-web.pdf.

34 Another element of Mr. Long's proposed model would be to amend the whistleblower rights section of the Act to include good faith disclosures of breaches as protected rights of employees.

organization that has suffered a security breach to notify credit bureaus about the breach and the individuals affected without the consent of those individuals. This would allow credit bureaus to be more proactive in protecting consumers from identity theft and fraud.

In her final appearance before the Committee, however, the Privacy Commissioner indicated that several recent major security breaches have generated an urgency to resolve this issue and as a result, the Commissioner is now recommending an amendment to PIPEDA to create a breach notification provision. Until such an amendment is made, the Commissioner will continue to work with stakeholders to develop voluntary guidelines. When questioned about her position on this issue by Committee Members, the Commissioner indicated that she did not feel that the introduction of an amendment to PIPEDA would greatly alter what is the current practice of organizations that are faced with a data security breach.

The Committee feels that there is a need for an amendment to PIPEDA to include a breach notification provision; however, we recognize that this will not be an easy task. We favour a model whereby organizations would be required to report breaches to the Privacy Commissioner, who would then conduct an analysis to determine whether or not notification should be made. Most critical in the development of a statutory breach notification model will be the necessary determination of threshold issues.

The Committee heard testimony that some form of standard should be established for notification that would take into consideration the nature and scope of the breach. For example, CIPPIC advocated for the California legislative model wherein the duty to notify is only triggered when there is an acquisition or reasonable belief of acquisition by an unauthorized person. It was felt that this standard is higher than mere access by an unauthorized person, but lower than a standard that requires notification if there is a risk of identity theft. The Canadian Bar Association recommended that a balanced privacy breach notification requirement be considered, such as a duty to notify only where an organization is not covered by security mechanisms (e.g. encryption or de-identification), or has received notice that such protection mechanisms have been breached and the information that has been compromised is sensitive personal information.

The Committee recognizes that the issue of threshold applies to two aspects of our recommended model: 1) the question of when organizations are required to report breaches to the Privacy Commissioner; and 2) the Commissioner's determination of whether or not there should be a notification. In determining the former threshold, we do not wish to see the Office of the Privacy Commissioner overburdened with breach reporting. Certainly, requiring notification to the Office of the Privacy Commissioner in every instance of a security breach may create an unworkable burden on that Office, and, at least, will have significant resource implications. We suggest that careful consideration be given to this issue in the development of a breach notification provision in PIPEDA.

Therefore, the Committee does not support what some refer to as "mandatory breach notification", in the sense of requiring that every person whose personal information

is compromised be notified in every case of a breach. We support requiring organizations to notify the Privacy Commissioner of certain defined security breaches, so that her office has an opportunity to assist in the determination of whether affected individuals should be notified, and if so, in what manner. This second stage of the process would be discretionary, in that the Privacy Commissioner would determine on a case by case basis whether or not to recommend notification.

In determining the specifics of an appropriate notification model for PIPEDA, the Committee believes that consideration should be given to threshold issues, such as under what conditions breaches of personal information holdings would be required to be reported to the Privacy Commissioner, as well as under what conditions the Privacy Commissioner would require notification of such reported breaches. There must also be consideration of questions of timing, manner of notification, penalties for failure to notify, and the need for a "without consent" power to notify credit bureaus in order to help protect consumers from identify theft and fraud.

Recommendation 23

The Committee recommends that PIPEDA be amended to include a breach notification provision requiring organizations to report certain defined breaches of their personal information holdings to the Privacy Commissioner.

Recommendation 24

The Committee recommends that upon being notified of a breach of an organization's personal information holdings, the Privacy Commissioner shall make a determination as to whether or not affected individuals and others should be notified and if so, in what manner.

Recommendation 25

The Committee recommends that in determining the specifics of an appropriate notification model for PIPEDA, consideration should be given to questions of timing, manner of notification, penalties for failure to notify, and the need for a "without consent" power to notify credit bureaus in order to help protect consumers from identity theft and fraud.

LIST OF RECOMMENDATIONS

Recommendation 1

The Committee recommends that a definition of "business contact information" be added to PIPEDA, and that the definition and relevant restrictive provision found in the Alberta *Personal Information Protection Act* be considered for this purpose.

Recommendation 2

The Committee recommends that PIPEDA be amended to include a definition of "work product" that is explicitly recognized as not constituting personal information for the purposes of the Act. In formulating this definition, reference should be added to the definition of "work product information" in the British Columbia *Personal Information Protection Act,* the definition proposed to this Committee by IMS Canada, and the approach taken to professional information in Quebec's *An Act Respecting the Protection of Personal Information in the Private Sector.*

Recommendation 3

The Committee recommends that a definition of "destruction" that would provide guidance to organizations on how to properly destroy both paper records and electronic media be added to PIPEDA.

Recommendation 4

The Committee recommends that PIPEDA be amended to clarify the form and adequacy of consent required by it, distinguishing between express, implied and deemed/opt-out consent. Reference should be made in this regard to the Alberta and British Columbia *Personal Information Protection Acts.*

Recommendation 5

The Committee recommends that the Quebec, Alberta and British Columbia private sector data protection legislation be considered for the purposes of developing and incorporating into PIPEDA an amendment to address the unique context experienced by federally regulated employers and employees.

Recommendation 6

The Committee recommends that PIPEDA be amended to replace the "investigative bodies" designation process with a definition of "investigation" similar to that found in the Alberta and British Columbia *Personal Information Protection Acts* thereby allowing for the collection, use and disclosure of personal information without consent for that purpose.

Recommendation 7

The Committee recommends that PIPEDA be amended to include a provision permitting organizations to collect, use and disclose personal information without consent, for the purposes of a business transaction. This amendment should be modeled on the Alberta *Personal Information Protection Act* in conjunction with enhancements recommended by the Privacy Commissioner of Canada.

Recommendation 8

The Committee recommends that an amendment to PIPEDA be considered to address the issue of principal-agent relationships. Reference to section 12(2) of the British Columbia *Personal Information Protection Act* should be made with respect to such an amendment.

Recommendation 9

The Committee recommends that PIPEDA be amended to create an exception to the consent requirement for information legally available to a party to a legal proceeding, in a manner similar to the provisions of the Alberta and British Columbia *Personal Information Protection Acts*.

Recommendation 10

The Committee recommends that the government consult with the Privacy Commissioner of Canada with respect to determining whether there is a need for further amendments to PIPEDA to address the issue of witness statements and the rights of persons whose personal information is contained therein.

Recommendation 11

The Committee recommends that PIPEDA be amended to add other individual, family or public interest exemptions in order to harmonize its approach with that taken by the Quebec, Alberta and British Columbia private sector data protection Acts.

Recommendation 12

The Committee recommends that consideration be given to clarifying what is meant by "lawful authority" in section 7(3)(c.1) of PIPEDA and that the opening paragraph of section 7(3) be amended to read as follows: "For the purpose of clause 4.3 of Schedule 1, and despite the note that accompanies that clause, an organization shall disclose personal information without the knowledge or consent of the individual but only if the disclosure is […]"

Recommendation 13

The Committee recommends that the term "government institution" in sections 7(3)(c.1) and (d) be clarified in PIPEDA to specify whether it is intended to encompass municipal, provincial, territorial, federal and non-Canadian entities.

Recommendation 14

The Committee recommends the removal of section 7(1)(e) from PIPEDA.

Recommendation 15

The Committee recommends that the government examine the issue of consent by minors with respect to the collection, use and disclosure of their personal information in a commercial context with a view to amendments to PIPEDA in this regard.

Recommendation 16

The Committee recommends that no amendments be made to PIPEDA with respect to transborder flows of personal information.

Recommendation 17

The Committee recommends that the government consult with members of the health care sector, as well as the Privacy Commissioner of Canada, to determine the extent to which elements contained in the PIPEDA Awareness Raising Tools document may be set out in legislative form.

Recommendation 18

The Committee recommends that the Federal Privacy Commissioner not be granted order-making powers at this time.

Recommendation 19

The Committee recommends that no amendment be made to section 20(2) of PIPEDA with respect to the Privacy Commissioner's discretionary power to publicly name organizations in the public interest.

Recommendation 20

The Committee recommends that the Federal Privacy Commissioner be granted the authority under PIPEDA to share personal information and cooperate in investigations of mutual interest with provincial counterparts that do not have substantially similar private sector legislation, as well as international data protection authorities.

Recommendation 21

The Committee recommends that any extra-jurisdictional information sharing, particularly to the United States, be adequately protected from disclosure to a foreign court or other government authority for purposes other than those for which it was shared.

Recommendation 22

The Committee recommends that PIPEDA be amended to permit the Privacy Commissioner to apply to the Federal Court for an expedited review of a claim of solicitor-client privilege in respect of the denial of access to personal information (section 9(3)(a)) where the Commissioner has sought, and been denied, production of the information in the course of an investigation.

Recommendation 23

The Committee recommends that PIPEDA be amended to include a breach notification provision requiring organizations to report certain defined breaches of their personal information holdings to the Privacy Commissioner.

Recommendation 24

The Committee recommends that upon being notified of a breach of an organization's personal information holdings, the Privacy Commissioner shall make a determination as to whether or not affected individuals and others should be notified and if so, in what manner.

Recommendation 25

The Committee recommends that in determining the specifics of an appropriate notification model for PIPEDA, consideration should be given to questions of timing, manner of notification, penalties for failure to notify, and the need for a "without consent" power to notify credit bureaus in order to help protect consumers from identity theft and fraud.

REQUEST FOR GOVERNMENT RESPONSE

Pursuant to Standing Order 109, the Committee requests that the government table a comprehensive response to this Report.

Respectfully submitted,

Tom Wappel, MP
Chairman

APPENDIX A
LIST OF WITNESSES

Organizations and Individuals	Date	Meeting
Department of Industry Michael Binder, Assistant Deputy Minister, Spectrum, Information Technologies and Telecommunications	2006/11/20	17
Department of Industry Danièle Chatelois, Privacy Policy Analyst, E-Commerce Policy Directorate, Electronic Commerce Branch	2006/11/20	17
Department of Industry Richard Simpson, Director General, Electronic Commerce	2006/11/20	17
Department of Justice Alexia Taschereau, Senior Counsel, Industry Canada	2006/11/20	17
As an Individual Colin Bennett, Political Science Professor, University of Victoria	2006/11/22	18
B.C. Freedom of Information and Privacy Association (FIPA) Richard Rosenberg, President	2006/11/22	18
Office of the Privacy Commissioner of Canada Jennifer Stoddart, Privacy Commissioner	2006/11/27	19
Office of the Privacy Commissioner of Canada Heather Black, Assistant Commissioner (PIPEDA)	2006/11/27	19
Office of the Privacy Commissioner of Canada Melanie Millar-Chapman, Strategic Research and Policy Analyst	2006/11/27	19
As an Individual Valerie Steeves, Department of Criminology, University of Ottawa	2006/11/29	20
Office of the Information and Privacy Commissioner of British Columbia David Loukidelis, Commissioner	2006/11/29	20
Canadian Marketing Association John Gustavson, President and Chief Executive Officer	2006/12/04	21
Canadian Marketing Association Wally Hill, Vice President, Public Affairs and Communications	2006/12/04	21

Organizations and Individuals	Date	Meeting
Canadian Marketing Association	2006/12/04	21
Barbara Robins, Vice-President, Legal and Regulatory Affairs, Reader's Digest		
Federally Regulated Employers - Transportation and Communication (FETCO)	2006/12/04	21
Don Brazier, Executive Director		
Federally Regulated Employers - Transportation and Communication (FETCO)	2006/12/04	21
Barbara Mittleman, Director, Employee Relations, Canadian Pacific Railway Company		
Federally Regulated Employers - Transportation and Communication (FETCO)	2006/12/04	21
Edith Cody-Rice, Senior Legal Counsel, Privacy Coordinator Canadian Broadcasting Corporation		
Canadian Internet Policy and Public Interest Clinic	2006/12/06	22
Philippa Lawson, Executive Director		
Marketing Research and Intelligence Association	2006/12/06	22
David Stark, MRIA Standards Chair		
Marketing Research and Intelligence Association	2006/12/06	22
Brendan Wycks, Executive Director		
Public Interest Advocacy Centre	2006/12/06	22
John Lawford, Counsel		
Public Interest Advocacy Centre	2006/12/06	22
Amanda Tait, Articling Student		
As an Individual	2006/12/11	23
Ian Kerr, Canada Research Chair in Ethics, Law and Technology, University of Ottawa		
Canadian Bar Association	2006/12/11	23
Brian Bowman, Chair, National Privacy and Access Law Section		
Canadian Bar Association	2006/12/11	23
Tamra Thomson, Director, Legislation and Law Reform		
Information Technology Association of Canada	2006/12/11	23
Bernard Courtois, President and Chief Executive Officer		
Information Technology Association of Canada	2006/12/11	23
Ariane Siegel, Lawyer		

Organizations and Individuals	Date	Meeting
Canadian Dental Association	2006/12/13	25
Wayne Halstrom, President		
Canadian Dental Association	2006/12/13	25
Andrew Jones, Director, Corporate and Government Relations		
Canadian Medical Association	2006/12/13	25
Bonnie Cham, Chair, Committee on Ethics		
Canadian Medical Association	2006/12/13	25
Jean Nelson, Assistant Director, Legal Services and Chief Privacy Officer		
Canadian Pharmacists Association	2006/12/13	25
Jeff Poston, Executive Director		
Canadian Bankers Association	2007/01/30	26
Terry Campbell, Vice-President, Policy		
Canadian Bankers Association	2007/01/30	26
Warren Law, Senior Vice-President, Corporate Operations and General Counsel		
Canadian Bankers Association	2007/01/30	26
Linda Routledge, Director, Consumer Affairs		
Credit Union Central of Canada	2007/01/30	26
Gary Rogers, Vice-President, Financial Policy		
Credit Union Central of Canada	2007/01/30	26
Charlene Loui-Ying, General Counsel and Government Relations Officer Credit Union Central of British Columbia		
Canadian Chamber of Commerce	2007/02/01	27
Michael Murphy, Executive Vice-President, Policy		
Canadian Chamber of Commerce	2007/02/01	27
Chris Gray, Policy Analyst		
Canadian Chamber of Commerce	2007/02/01	27
David Elder, Vice-President, Regulatory Law, Bell Canada		

Organizations and Individuals	Date	Meeting
Canadian Life and Health Insurance Association Inc. Yves Millette, Senior Vice-President, Quebec Affairs	2007/02/01	27
Canadian Life and Health Insurance Association Inc. Dale Philp, Assistant Vice-President and Senior Counsel , Sun Life Financial	2007/02/01	27
Canadian Life and Health Insurance Association Inc. Frank Zinatelli, Vice-President and Associate General Counsel	2007/02/01	27
Dominion of Canada General Insurance Company Vivian Bercovici, Counsel	2007/02/06	28
Dominion of Canada General Insurance Company Ann MacKenzie, Privacy Officer	2007/02/06	28
Insurance Bureau of Canada Randy Bundus, Vice-President, General Counsel and Corporate Secretary	2007/02/06	28
Insurance Bureau of Canada Mark Yakabuski, Vice-President, Federal Affairs and Ontario	2007/02/06	28
Murray Long & Associates Murray Long, President	2007/02/06	28
IMS Health Canada Gary Fabian, Vice-President, Public Affairs and Corporate Relations	2007/02/08	29
IMS Health Canada Anita Fineberg, Corporate Counsel and Chief Privacy Officer, Canada and Latin America	2007/02/08	29
IMS Health Canada Léo-Paul Landry, Member, Medical Advisory Board	2007/02/08	29
National Association for Information Destruction - Canada Dave Carey, Chair	2007/02/08	29
National Association for Information Destruction - Canada Robert Johnson, Executive Director	2007/02/08	29
Canadian Association of Chiefs of Police Clayton Pecknold, Co-Chair, Law Amendments Committee	2007/02/13	30

Organizations and Individuals	Date	Meeting
Canadian Resource Centre for Victims of Crime	2007/02/13	30
Steve Sullivan, President		
Canadian Resource Centre for Victims of Crime	2007/02/13	30
Krista Gray-Donald, Director of Research		
Insurance Brokers Association of Canada	2007/02/13	30
Robert Kimball, Chairman		
Insurance Brokers Association of Canada	2007/02/13	30
Peter Fredericks, Vice-President		
Insurance Brokers Association of Canada	2007/02/13	30
Steve Masnyk, Manager of Communications		
Canadian Federation of Independent Business	2007/02/15	31
Lucie Charron, Policy Analyst		
Canadian Federation of Independent Business	2007/02/15	31
Corinne Pohlmann, Director, National Affairs		
Consumers' Association of Canada	2007/02/15	31
Margaret Anne Ireland, Director		
Royal Canadian Mounted Police	2007/02/20	32
Bruce Rogerson, Assistant Commissioner		
Royal Canadian Mounted Police	2007/02/20	32
Art Crockett, Officer in Charge, Strategic Services Branch,Technical Operations		
Royal Canadian Mounted Police	2007/02/20	32
Earla-Kim McColl, Superintendent, National Child Exploitation Coordination Centre		
Office of the Privacy Commissioner of Canada	2007/02/22	33
Jennifer Stoddart, Privacy Commissioner		
Office of the Privacy Commissioner of Canada	2007/02/22	33
Heather Black, Assistant Commissioner (PIPEDA)		

APPENDIX B
LIST OF BRIEFS

Organizations and individuals

Advocis

Association of Canadian Archivists

B.C. Freedom of Information and Privacy Association (FIPA)

Burbidge, **Scott**

Canada Health Infoway

Canadian Bankers Association

Canadian Bar Association

Canadian Chamber of Commerce

Canadian Dental Association

Canadian Internet Policy and Public Interest Clinic

Canadian Life and Health Insurance Association Inc.

Canadian Marketing Association

Canadian Real Estate Association

Canadian Resource Centre for Victims of Crime

Credit Union Central of Canada

Federally Regulated Employers - Transportation and Communication (FETCO)

Federation of Medical Regulatory Authorities

IMS Health Canada

Information Technology Association of Canada

Insurance Bureau of Canada

Organizations and individuals

Kerr, **Ian**

Mouvement des caisses Desjardins

Murray Long & Associates

Mutual Fund Dealers Association of Canada

National Association for Information Destruction - Canada

Office of the Information and Privacy Commissioner of British Columbia

Office of the Privacy Commissioner of Canada

Public Interest Advocacy Centre

Royal Canadian Mounted Police

Speers, **Richard**

House of Commons Standing Committee on Access to Information, Privacy and Ethics (the "Committee")

Statutory Review of the *Personal Information Protection and Electronic Documents Act* (2000, c. 5) ("PIPEDA"): **DISSENTING OPINION**

The Conservative members of Committee acknowledge the thoughtful participation of the many individuals and groups who appeared as witnesses and/or presented submissions during the review. The majority report includes many constructive recommendations for technical changes, however, the Conservative members of the Committee dissent with recommendation 14 to repeal section 7(1)(e) of PIPEDA.

1.0 Listening to Small Business

As noted in the majority report, PIPEDA only fully came into effect on January 1, 2004. The Conservative members wish to emphasize the majority report's focus on fine-tuning PIPEDA, rather than prescribing wholesale changes. The business community, privacy stakeholders and officials, including the Office of Privacy Commissioner of Canada, are facilitating PIPEDA's adoption. The Conservative members of the Committee support those efforts. The Conservative members do not support efforts that would unduly increase the compliance burden on the small business community through, for example, changes that would make PIPEDA unnecessarily prescriptive. The Conservative members applaud the work of those business groups, including the Canadian Federation of Independent Business, helping small and medium-sized businesses comply with PIPEDA and protect Canadians' personal information.

2.0 Dissent

The Conservative members respectfully dissent from recommendation 14 of the majority report, and the reasons given at paragraphs 79 through 85 of the majority report.

Section 7(1)(e) allows organizations to collect and use information related to national security, defence, or international affairs. The previous Liberal government included this section in PIPEDA for the express purpose of closing legislative gaps relating to transportation and national security, specifically air travel. The Conservative members of Committee believe the removal of section 7(1)(e) could threaten the safety of Canada's civil aviation system.

3.0 Inappropriate Timing

The majority's reconsideration of section 7(1)(e) is premature. The section was adopted as part of the *Public Safety Act*, 2002 (2004, c. 15), and only came into force in May 2004. Arguably, section 7(1)(e) is not properly within the ambit of this statutory review. By mandating a five (5) year review, the drafters of PIPEDA determined stakeholders ought to actually benefit from five (5) years of experience before reflecting the efficacy of the legislation. Section 7(1)(e) was not part of the original legislation, so affected stakeholders have not benefited from five (5) years of experience with the provision.

4.0 No Stakeholder Input Before the Committee

The *Public Safety Act* was the product of an attempt to balance public safety and individual privacy. In contrast, the majority report recommends repealing part of the *Public Safety Act* without any input from the affected stakeholders, including airlines, airports, air passenger groups or security agencies. Recommendation 14 and paragraphs 79-85 of the majority report are completely devoid of input from the stakeholders most affected by the recommendation.

The Conservative members of the Committee note that, notwithstanding any comments in the majority report, the Honourable Stockwell Day, Minister of Public Safety and Emergency Preparedness, replied to the Committee in a letter dated April 19, 2007. The Conservative members of the Committee appreciate the input of the Minister on sections 7(1)(e) and 9. The Conservative members of the Committee also welcome the Minister's interest in clarifying section 7(3)(c.1). Minister Day's letter is attached as an annex to this dissenting opinion.

4.0 Conclusion

The Conservative members vigorously dissent from the majority's recommendation to weaken Canada's national security laws; a recommendation made by the Liberal and New Democrat members without any input or representation from the security or air transportation communities.

Minister of Public Safety
and Emergency Preparedness

Ministre de la Securite publique
et de la Protection civile

Ottawa, Canada K1A OP8

19 APR 2007

Mr. Tom Wappel, M.P.
Chairman
Standing Committee on
Access to Information, Privacy and Ethics
House of Commons
Ottawa, Ontario KIA OA6

Re: Statutory Review of the Personal Information Protection and Electronic Documents Act (PIPEDA)

Dear Mr. Wappel

Thank you for your letter of March 20, 2007. I appreciate the opportunity to contribute to the House of Commons Standing Committee on Access to Information, Privacy and Ethics' important work in conducting a statutory review of the *Personal Information Protection and Electronic Documents Act* (PIPEDA).

You requested my views on s. 7(1) (e) of PIPED A, which was added to PIPEDA by the *Public Safety Act.*

Subsection 7(1)(e) provides that an organization may collect personal information without the knowledge or consent of the individual if the collection is made for the purposes of a disclosure required by law or a disclosure to the government, where the information relates to national security, defence, or international affairs and is either requested by a government institution that has lawful authority to obtain it, or on the organization's own initiative.

Part of the objective of subsection 7(1)(e), as part of the *Public Safety Act* (which received Royal Assent on May 6,2004), is to improve Canada's capacity to provide a secure environment, in particular for transportation and air travel. The Act closes legislative gaps relating to transportation and national security by amending existing laws, such as the *Aeronautics Act,* the *Criminal Code,* the *Canadian Air Transport Security Authority Act,* and others, as well as PIPEDA.

The amendments to the *Aeronautics Act* in particular were designed to grant the authority to request, and use, passenger information to protect the security of the country and its aviation system. The amendments to PIPEDA s.7 (1) (e) and 7(2) (d) were consequential amendments needed to ensure that the provisions of PIPEDA did not conflict with the *Public Safety Act.*

It should also be noted that an important goal of the *Public Safety Act* is to balance the interest of public safety and individual privacy, and a number of safeguards were included in the law to achieve this, while ensuring transparency and accountability. The proposals were the subject of extensive consultations, and a lengthy review in Parliament. Many changes were made throughout this process to address comments and concerns expressed by various stakeholders, including the Office of the Privacy Commissioner and, as a result, the amendments to PIPEDA provided for under s. 98 of the *Public Safety Act* are limited in scope and narrowly targeted to achieve their goals.

Given the above, I am concerned about the impact that changes suggested by witnesses to the previous PIPEDA amendments, enacted pursuant to the *Public Safety Act,* could have on achieving the goals of the *Public Safety Act* and, as a consequence, on public safety.

Strong safeguards in relation to law enforcement activities are already enshrined in legislation such as Police Acts and the *Criminal Code,* to review the actions of the police when collecting and using personal information. In addition, the court system oversees the results of police work and ensures, in applying the laws of evidence, as well as the *Charter of Rights and Freedoms,* that police collection of information is done appropriately.

As you know, PIPEDA was enacted to protect the privacy of information being held by private companies and was never intended to impede police work. However, the current wording of section 7 and section 9 of PIPEDA has led to confusion among the private sector as to how and whether they can cooperate with the police, which should be remedied.

<u>Section 7:</u>

Subsection 7(3)(c.1) states that an organization may disclose personal information without the knowledge or consent of the individual if the government institution has lawful authority to obtain the requested information. Unfortunately, the phrase "lawful authority" has been misinterpreted by some private sector organizations as an obligation to obtain judicial authorization before releasing any information to police and security agencies.

While the language of s. 7(3)(c), which refers to subpoenas and warrants, can clearly be considered to preclude such an interpretation oflawful authority under s.7(3)(c.!), the reality is that the lack of a definition of lawful authority has resulted in an ambiguity, which is in many instances posing a problem for police.

A requirement to obtain a warrant was never intended, nor would it be practical, given the broad definition of personal information. This misinterpretation can result in an inability for police to obtain even basic information needed for general policing functions to assist the public. A troubling example of the potential negative impact of a misinterpretation of this provision is seen in the context of an Internet Service Provider refusing to provide urgently necessary contact information on a subscriber to the police in a situation where a child is being lured in real-time in a chat room by an online predator.

Given the above challenges resulting from the lack of clarity as to what constitutes "lawful authority", I believe that this section, in particular the term "lawful authority", would benefit from clarification.

Section 9:

Section 9 of PIPEDA is also causing law enforcement agencies some concern, due to a possible loophole in the provision designed to protect police investigations. PIPEDA provides that an individual shall be given access to personal information about themselves and have a right to be informed about the disclosure of any of their personal information. To protect investigations, section 9 of PIPED A provides an exception whereby law enforcement agencies can object and thereby prohibit an organization from revealing to an individual that a request has been received from or disclosure of information has been provided to a law enforcement agency.

Section 9, however, does not address the situation where an organization chooses voluntarily to disclose to an individual a police request for information. Significant harm can result to ongoing police investigations if an organization voluntarily discloses to an individual that he or she is under investigation. For example, this individual or group could then proceed to destroy evidence before the police could intercede.

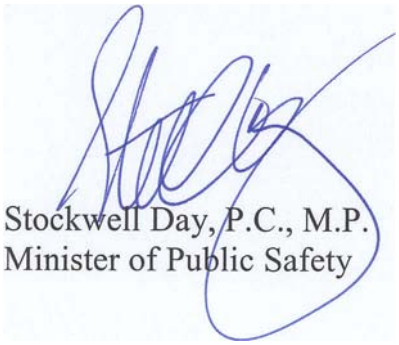
It is therefore important to police investigations that section 9 be clarified to ensure that organizations are prohibited from disclosing the existence of an investigation or the fact that the police had made any inquiries regardless of

whether an individual has made a request for this information or the organization wishes to voluntarily notify the individual.

I recently wrote to my colleague, the Honourable Maxime Bernier, Minister of Industry, to advise him of the challenges the police have experienced with respect to PIPEDA. I have attached a copy of my letter to him for your reference.

Thank you again for the opportunity to contribute to the Committee's work in reviewing this important piece of legislation.

Yours sincerely,



Stockwell Day, P.C., M.P.
Minister of Public Safety

Bloc Québécois Dissenting Report
April 23, 2007

The Bloc Québécois played an active and responsible role in the study of Part I of the *Personal Information Protection and Electronic Documents Act* (PIPEDA). Although we had suggested a number of amendments to "limit the damage," the Bloc Québécois wishes to reiterate its complete disagreement with this act, which was adopted in 2000 and was widely criticized by the Government of Québec, businesses, consumers, the Québec Employers' Council, editorial writers, constitutional experts, etc.

PIPEDA: an example of raiding by the federal government

Let us recall that the PIPEDA was passed during the controversy in the late 1990s, when Bill C-6[1] received royal assent. The Government of Québec and the provinces argued essentially that while the federal government claimed legitimacy for the PIPEDA pursuant to its jurisdiction over the regulation of trade and commerce, the protection of personal information falls under the jurisdiction of Québec and the provinces by virtue of the constitutional power over property and civil rights. In this regard, a constitutional expert from Québec noted:

> *"In my opinion, Bill C-54 violates the letter and the spirit of the division of powers as it must be understood in this country. It takes an arrogant and intrusive approach to provincial areas of jurisdiction. […] The protection of privacy is essentially a matter of provincial jurisdiction. In Québec, for instance, property and civil rights, the Civil Code and the Québec act apply, in addition to the Canadian and Québec charters."*
>
> Jacques Frémont, constitutional expert, Université de Montréal

In Québec, personal information is protected

The federal act merely overlaps with existing provisions in Québec:

- The *Act Respecting the Protection of Personal Information in the Private Sector* has protected personal information in Québec since 1993;
- The *Québec Charter of Rights* explicitly states in section 5 that every person has the right to privacy;
- The *Civil Code* (Chapter 3, especially sections 36 to 40) includes provisions regarding the protection of privacy.

Moreover, businesses under federal jurisdiction with dealings in Québec were already covered by the Québec act. Québeckers' right to the protection of privacy is protected by the Québec act, whether in dealings with a business under provincial or federal jurisdiction. The Task Force on the Future of the Canadian Financial Services Sector devoted an entire volume to the protection of personal

1 C-6 replaced Bill C-54, which died on the Order Paper in September 1999.

information in this sector, written by Richard Owen and published last September. It states:

> *"*On a literal reading, the Act applies to banks as well as other financial institutions. *(…) In the absence of federal legislation on a particular subject matter, validly enacted provincial law may apply to a federal undertaking unless the law prevents the federal undertaking from managing its operations or generally accomplishing its ends."*[2]

Moreover, the report states that Québec law already applied to interprovincial and international trade as well.

> "Moreover, the effects of the Québec Act will not be confined to the province. National institutions will face the Act's restriction on the extra-provincial transfer of information (about Québec residents)."[3]

The PIPEDA gives the federal government the power to render a Québec law invalid

The federal act applies to all financial activities unless the Governor in Council orders, if satisfied that a province has adopted similar legislation, that it be exempted in whole or in part.

In December 2003, the federal government issued an exclusion order[4] applicable to organizations in Québec. Unfortunately, not only is the power set out in paragraph 26(2)b[5] left to the government's sole discretion, but it applies only to information within Québec and held by companies under provincial jurisdiction.

Pursuant to this paragraph, the Governor in Council could therefore if it wishes order that the laws of Québec be declared partially or wholly invalid, without even referring the matter to Parliament. This is unacceptable to the Bloc Québécois.

---

2 Task Force on the Future of the Canadian Financial Services Sector. *Privacy and Financial Services in Canada,* Owens, Richard, September 1998, p. 79-80

3 Op. cit. , p. 82

4 http://canadagazette.gc.ca/partII/2003/20031203/html/sor374-e.html

5 26(2)(*b*) if satisfied that legislation of a province that is substantially similar to this Part applies to an organization, a class of organizations, an activity or a class of activities, exempt the organization, activity or class from the application of this Part in respect of the collection, use or disclosure of personal information that occurs within that province.