Statutory Review of the *Personal Information Protection and Electronic Documents Act*

Submission to the House of Commons Standing Committee on Access to Information, Privacy and Ethics

November 29, 2006

David Loukidelis
Information & Privacy Commissioner for British Columbia

Mailing Address: PO Box 9038, Stn Prov Govt, Victoria B.C. V8W 9A4
Location: Third Floor, 756 Fort Street
Telephone: (250) 387-5629 Facsimile: (250) 387-1696
Toll Free enquiries through *Enquiry BC* at (800) 663-7867 or (604) 660-2421 (Vancouver)
website: http//www.oipc.bc.ca

PREFACE

British Columbia's *Personal Information Protection Act* has been in force since January 1, 2004.[1] Since then, the Office of the Information and Privacy Commissioner for British Columbia has acquired considerable experience in enforcing compliance and in assisting private sector organizations, both for-profit and not-for-profit, in complying with the law. The goal of this document is to discuss selected issues through the lens of our experience in order to assist Parliament with the statutory review of the *Personal Information Protection and Electronic Documents Act*.[2] In doing so, this document touches on issues raised in the discussion paper issued by my federal colleague, Jennifer Stoddart, last summer.[3]

Victoria, British Columbia

November 29, 2006

David Loukidelis
Information and Privacy Commissioner
for British Columbia

1.0 INTRODUCTION

Canada's privacy laws incorporate internationally-accepted fair information principles that are reflected in privacy laws throughout the world and in international instruments.[4] Applying these principles, our privacy laws aim to give individuals a degree of control over their own personal information throughout its life cycle. They give individuals the right to be told what information is being collected about them, who is collecting it, the uses to which it will be put, to whom it might be disclosed, and for what purposes it might be used or disclosed. Our private sector privacy laws also enable individuals to generally choose which information to disclose and for what purposes.

Information each year becomes more and more important to government, notably for service delivery, immigration, law enforcement and national security purposes. Personal information travels the globe on the new Spice Routes and these flows of information are increasingly important to commerce and economic development.[5] New information technologies are transforming how personal information is collected, used and disclosed. Year in and year out, opinion polls speak loud and clear to Canadians' disquiet about risks to their privacy. They have some reason to be concerned and can legitimately demand, as a matter of principle, that their reasonable privacy expectations be protected. Moreover, their privacy concerns can influence behaviour in ways that have real economic costs.[6] For these and other reasons, it is critically important that, in our increasingly interdependent and networked world our privacy laws be strong enough to meet present and approaching privacy risks.

Canada's private sector privacy laws offer reasonable privacy protections to individuals while protecting the reasonable interests of businesses and other private sector organizations. Because they are all founded on internationally-accepted fair information principles they have a very great deal in common. They are in every important respect harmonious, not a patchwork.[7] Other countries—notably the United States[8]—have multiple privacy laws and Canada's approach to private sector privacy compares very well against the experience elsewhere. The substantial similarity of our privacy sector privacy laws makes it safe to say that, generally speaking, an organization that complies with the *Personal Information Protection and Electronic Documents Act* ("PIPEDA") will likely be in compliance with, for example, British Columbia's *Personal Information Protection Act* ("PIPA").[9]

Another advantage to Canadians of having provincial private sector privacy laws is that they protect the privacy interests of employees in the provincially-regulated workplace. PIPEDA does so in the federally-regulated sector, but Parliament cannot constitutionally legislate in respect of the employment relationship. It could not, therefore, legislate privacy in the provincially-regulated sector.[10] This remains the case, although in times of national emergency, federal legislation respecting or affecting labour and employment has been upheld.[11]

2.0 DISCUSSION

2.1 Technological Neutrality is Important—Concerns occasioned by the rise of computerized databases in the 1960s contributed greatly to the development of modern privacy laws. Information technologies can offer benefits for privacy, *e.g.,* through encryption of personal information or use of computerized audit trails that enable system operators to automatically identify inappropriate access to or use of personal information. Nonetheless, rapid advances in information technologies will continue to present significant challenges for privacy in both the public and private sectors. For example, analysis of increasingly large databases of personal information using techniques generally known as data mining can often yield benefits, but can equally raise privacy risks. It is nonetheless vitally important that privacy laws remain current and capable of addressing these risks.

Canadian privacy laws are overwhelmingly technology-neutral. PIPA does prescribe technological solutions for privacy risks or otherwise specifically address technological risks. PIPA does not, for example, require organizations to implement specific technologies in order to protect personal information using reasonable security measures. Instead, PIPA requires organizations to protect personal information using "security safeguards appropriate to the sensitivity of the information".[12] By imposing an objective standard of reasonableness for protective safeguards, PIPA ensures that, as both technological threats and solutions evolve, the legislation can be applied in light of what is reasonable at the relevant time. This forward-looking approach should continue.

2.2 Cross-Border Cooperation—The globalization of personal information flows associated with commercial and government activities challenges national sovereignty and law-making authority.[13] Given this, if privacy commissioners and other data protection authorities are to do their jobs properly, they need the necessary tools to cooperate with each other.

PIPEDA authorizes the Privacy Commissioner of Canada to enter into consultations with other Canadian privacy commissioners and to enter into agreements with them to coordinate activities of their offices, "including to provide for mechanisms for the handling of any complaint in which they are mutually interested".[14] In January 2004, my office, the office of the federal Privacy Commissioner and the office of the Information and Privacy Commissioner of Alberta entered into a cooperative arrangement for coordination of our activities. This arrangement is working well. Under it, our offices co-ordinate investigation activities on specific complaints, conduct joint investigations and share information on interpretation and application of these three very similar laws.

The federal Commissioner should also, in my view, have explicit authority for cooperative investigation, enforcement and other activities with privacy commissioners and data protection authorities outside Canada, particularly in the

Asia-Pacific region, the United States and the European Union. This is vital in order to protect the privacy of British Columbians and other Canadians in a networked global economy and a world of increasing trans-border information-sharing by governments and their agencies.

2.3 Work Product and Personal Privacy—Private sector privacy laws are designed to protect information about identifiable individuals. Some of the information that organizations collect or compile is not necessarily about a person as an individual in any generally-accepted sense. 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.

For this reason, PIPA's privacy protections do not apply to "work product information". This is achieved by excluding "work product information" from "personal information" protected by PIPA:

> **"work product information"** means 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.

This provides clarity and certainty for both organizations and individuals about what information is covered by PIPA's rules on collection, use and disclosure.

An example from the employment setting illustrates this. If an employee were to make a request under PIPA to her former employer for access to "all emails that I ever sent or received while working for you", it would not be necessary for the employer to respond simply because the former employee is mentioned as the author or recipient of an email. If the information in the emails was prepared or collected by the former employee as part of her responsibilities or activities related to her employment, the content of the emails would not be her personal information and the right of access under PIPA would not apply.

2.4 Employment Privacy—PIPA contains a special set of rules for employers' collection, use and disclosure of employee personal information for certain employment-related purposes.[15] These special rules form a code for "employee personal information". The main feature is that employee consent to collection, use and disclosure is not required.

If PIPA did not contain these rules, employers would have to obtain the consent of their employees for collection, use and disclosure of personal information for employment-related purposes, even where it would be neither appropriate nor practicable to get consent. For example, it would be neither practicable nor

appropriate to seek consent to covert observation from an employee whom the employer reasonably suspects of stealing company property.

PIPA defines employee personal information as follows:

> **"employee personal information"** means personal information about an individual that is collected, used or disclosed solely for the purposes reasonably required to establish, manage or terminate an employment relationship between the organization and that individual, but does not include personal information that is not about an individual's employment

PIPA's definition of employee personal information contains an easy-to-administer four-part test:

1. The information must be "personal information", *i.e.*, "information about an identifiable individual",

2. The personal information must be collected, used or disclosed "for the purposes reasonably required" to establish, manage or terminate an employment relationship,

3. The personal information must be collected "solely" for those purposes, and

4. The personal information must not be "personal information that is not about an individual's employment".[16]

The employee personal information rules apply only to personal information that meets the above conditions PIPA further provides that employers can only collect, use or disclose employee personal information where it is "reasonable" to do for purposes of establishing, managing or terminating an employment relationship with the individual.[17] So, although PIPA does not require employee consent to collection, use and disclosure of employee personal information, an employer does not have a completely free hand. The employer must be able to demonstrate that its collection, use and disclosure of employee personal information are reasonable in the circumstances of the case.

Our experience under PIPA demonstrates that the employee personal information rules appropriately balance the interests of employers and the interests of employees regarding privacy in the workplace. They have a further advantage. They enable consistency of interpretation and application across the labour force and economy, which is both desirable in principle and efficient. This is because PIPA's language allows the rules to be interpreted and applied across the non-unionized and unionized workforce in a manner that is consistent with principles developed by labour arbitrators in the unionized workplace.

2.5 Business Transactions—Another feature of PIPA that enjoys widespread support is the set of rules permitting the transfer of personal

information, subject to certain conditions, in the course of the sale of a business.[18] Without those rules, consent of each customer or employee of a business would be necessary before that business could disclose customers' personal information to a prospective purchaser of the business.[19]

PIPA authorizes an organization to disclose, without consent and subject to conditions, personal information about its employees, customers, management and shareholders to another party in connection with the sale of the organization or substantial assets of the organization. Disclosure is permitted only where the other party needs the personal information to determine whether to proceed with the business transaction.[20] PIPA also requires that notice be given to the employees, customers, management and shareholders of the affected organization that the business transaction has occurred and that their personal information has been disclosed to the acquiring party.[21]

If the transaction proceeds, the organization may disclose the personal information to the acquiring organization, which may then use or disclose the personal information only for the "same purposes for which it was collected, used or disclosed by the organization" and only where the personal information "relates directly to the part of the organization or its business assets that is covered by the transaction".

These rules facilitate the buying and selling of businesses without compromising individual privacy. They are both workable and efficient.

3.0 CONCLUSION

Again, this document only touches on selected issues that may be of interest for Parliament's review of PIPEDA. If members of the Standing Committee have questions, I would be pleased to assist in any way I can today or afterward.

---

[1] British Columbia's *Personal Information Protection Act* will undergo its own statutory review over the coming year. A statutory review of Alberta's *Personal Information Protection Act* is now underway.

[2] The views expressed in this document are not the views of the British Columbia government or anyone else other than its author.

[3] Office of the Privacy Commissioner of Canada, *Protecting Privacy in an Intrusive World* (July 2006). http://www.privcom.gc.ca/information/pub/pipeda_review_060718_e.pdf

[4] See, for example, the OECD's 1980 *Guidelines on the Protection of Privacy & Transborder Flows of Personal Data* and APEC's *Privacy Framework* of 2004. Canada has signed on to both of these.

[5] This evocative term has been used by Joseph Alhadeff, Chief Privacy Officer and Vice-President Global Public Policy, Oracle Corporation.

[6] "Forget the Grinch: Security & Privacy Concerns Are Stealing Canadians Away from Online Shopping", E-ChannelNews.com, November 20, 2006, http://www.e-channelnews.com/ec_storydetail.php?ref=413187. Just last week, for example, another opinion poll concluded that many Canadian consumers remain reluctant to shop online because of their privacy and security fears.

[7] PIPA has been recognized by the federal Cabinet as substantially similar to PIPEDA, as have Quebec's *An Act Respecting the Protection of Personal Information in the Private Sector*,

Alberta's *Personal Information Protection Act* and Ontario's *Personal Health information Protection Act*.

[8] There are many federal and state privacy laws in the United States that apply to various sectors. Examples from the federal level alone include the Gramm-Leach-Bliley Act (financial privacy), the *Health Insurance Portability and Accountability Act* (health privacy), the *Telecommunications Privacy Act*, the *Driver's Licensing Privacy Act* and the *Children's Online Privacy Protection Act*.

[9] For a copy of PIPA, see http://www.qp.gov.bc.ca/statreg/stat/P/03063_01.htm.

[10] See *Toronto Electric Commissioners v. Snider et al*, [1925] 2 D.L.R. 5, [1925] A.C. 396 (P.C.).

[11] See, most recently, *Re Anti-Inflation Act*, [1976] 2 S.C.R. 373.

[12] PIPEDA refers to s. 5(1) and Schedule 1, principle 4.7. A similar approach is taken under s. 34 of PIPA.

[13] This is acknowledged by international instruments such as the OECD *Guidelines on the Protection of Privacy and Transborder Flows of Personal Data Flows* and the APEC *Privacy Framework*, which attempt to harmonize privacy laws in order to adequately protect privacy while not unnecessarily impeding cross-border flows of data.

[14] PIPEDA, s. 23.

[15] Alberta has similar provisions under its *Personal Information Protection Act*. For a copy of Alberta's law, see http://www.qp.gov.ab.ca/documents/Acts/P06P5.cfm?frm_isbn=0779726316.

[16] Order P06-04, [2006] B.C.I.P.C.D. No. 35, para. 38.

[17] PIPA, ss. 13, 16 and 19.

[18] PIPA, s. 20.

[19] Much would depend on the nature of the customer's consent. For example, the organization may have obtained consent, when the customer signed up for a service, to disclosure for such purposes. This will not always be the case, but this is a plausible scenario.

[20] The disclosing organization and the receiving party also must enter into an agreement requiring the other party to use and disclose the personal information only for purposes related to the prospective business transaction. If the transaction does not complete, the receiving party must destroy the personal information or return it to the disclosing organization.

[21] Alberta's law does not require that notice be given. Alberta PIPA, s. 22.