THE LEGISLATIVE ASSEMBLY OF
BRITISH COLUMBIA

STREAMLINING BRITISH COLUMBIA'S PRIVATE SECTOR PRIVACY LAW

SPECIAL COMMITTEE TO REVIEW THE PERSONAL INFORMATION PROTECTION ACT

REPORT

FOURTH SESSION, THIRTY-EIGHTH PARLIAMENT

APRIL 2008

National Library of Canada Cataloguing in Publication Data

British Columbia. Legislative Assembly. Special Committee to Review the Personal Information Protection Act.
Streamlining British Columbia's private sector privacy law

At head of title: The Legislative Assembly of British Columbia.
"Report. Fourth Session, Thirty-Eighth Parliament."
ISBN 978-0-7726-5983-5

1. British Columbia. Personal Information Protection Act. 2. Privacy, Right of - British Columbia. 3. Business records - Law and legislation - British Columbia. 4. Data protection - Law and legislation - British Columbia. I. Title. II. Title: Report. III. Title: Special Committee to Review the Personal Information Protection Act report.

KEB505.62.B74 2008 342.71'0858 C2008-960088-6
KF5753.I5B74 2008

Office of the Clerk of Committees

SPECIAL COMMITTEE TO REVIEW THE PERSONAL INFORMATION PROTECTION ACT

Location:
Room 224, Parliament Buildings
Victoria, British Columbia
V8V 1X4

Telephone: **(250) 356-2933**

Toll free at: **1-877-428-8337**

Fax: **(250) 356-8172**

Email: **ClerkComm@leg.bc.ca**

Internet Homepage:
This report and others are available at our Internet homepage which also contains further information about this and other Select Standing and Special Committees: www.leg.bc.ca/cmt

April 17, 2008

To the Honourable
Legislative Assembly of the
Province of British Columbia

Honourable Members:

I have the honour to present herewith the Report of the Special Committee to Review the Personal Information Protection Act.

The Report covers the work of the Special Committee from May 7, 2007 to April 15, 2008.

Respectfully submitted on behalf of the Committee,

Ron Cantelon, MLA
Chair

TABLE OF CONTENTS

COMPOSITION OF THE COMMITTEE

MEMBERS

Ron Cantelon, MLA	Chair	Nanaimo-Parksville
Harry Lali, MLA	Deputy Chair	Yale-Lillooet
Leonard Krog, MLA		Nanaimo
Mary Polak, MLA		Langley
John Rustad, MLA		Prince George-Omineca

CLERK TO THE COMMITTEE

Kate Ryan-Lloyd, Clerk Assistant and Committee Clerk

Craig James, Clerk Assistant and Clerk of Committees

COMMITTEE RESEARCHERS

Josie Schofield, Committee Research Analyst

Assisted by Naomi Adams (fall 2007) and Simon Gray-Schleihauf (summer 2007)

TERMS OF REFERENCE

On February 19, 2008, the Legislative Assembly agreed that a Special Committee to Review the *Personal Information Protection Act* be appointed to examine in accordance with section 59 of the *Personal Information Protection Act* (SBC 2003, c. 63) and in particular, without limiting the generality of the foregoing, the collection, use and disclosure of personal information by organizations.

The Special Committee so appointed shall have the powers of a Select Standing Committee and is also empowered:

(a) to appoint of their number, one or more subcommittees and to refer to such subcommittees any of the matters referred to the Committee;

(b) to sit during a period in which the House is adjourned, during the recess after prorogation until the next following Session and during any sitting of the House;

(c) to adjourn from place to place as may be convenient; and

(d) to retain such personnel as required to assist the Committee,

and shall report to the House as soon as possible, but no later than April 19, 2008, or following any adjournment, or at the next following Session, as the case may be; to deposit the original of its reports with the Clerk of the Legislative Assembly during a period of adjournment and upon resumption of the sittings of the House, the Chair shall present all reports to the Legislative Assembly.

The said Special Committee is to be comprised of the following members: Mr. *Cantelon,* Convener; Ms. *Polak,* Mr. *Rustad*, and Messrs*. Lali and Krog.*

EXECUTIVE SUMMARY

British Columbia's private-sector privacy law came into force on January 1, 2004. In April 2007, the all-party Special Committee to Review the Personal Information Protection Act was appointed to conduct the first statutory review. During the past year the Committee received 39 submissions.

The key findings from our consultations are:

- At this stage of its development, the Act seems to be working well overall for private-sector organizations operating in British Columbia.
- The Act also aligns well with the federal and Alberta private-sector privacy laws.
- While large corporations and not-for-profit organizations based in BC have a good grasp of the legislation, the public is not as aware of the purpose, rules and scope of the Act.

This report contains 31 recommendations designed to fill gaps and streamline certain provisions of the Personal Information Privacy Act (PIPA) to facilitate consistency with other privacy laws.

KEY RECOMMENDATIONS

Enhance accountability for cross-border data flows

Require private-sector organizations operating in BC to be responsible for the personal information they transfer to a third party for processing outside Canada (Recommendation 1).

Require mandatory notification of privacy breaches in certain circumstances

Include in the Act an express duty for organizations to notify affected individuals of certain privacy breaches related to unauthorized disclosure or use of sensitive financial or health information (Recommendation 2).

Ban the use of blanket consent forms by provincially regulated financial institutions

Include in the Act a clause that prohibits blanket consent across financial pillars, and review PIPA for consistency with credit-reporting requirements in *Business Practices and Consumer Protection Act* (Recommendation 10).

Revise consent exceptions to better address business practices in the insurance industry

Add a clause to sections 12, 15 and 18 of the Act to allow the collection, use and disclosure without consent of personal information necessary for the insurer to assess, adjust, settle or litigate a claim under an insurance policy (Recommendation 11).

Permit disclosure of personal contact information for health research

Replace section 21(1)(b) of the Act with a provision stating that personal information can only be disclosed for research contact purposes with the approval of the Commissioner according to criteria set out in the Act or by regulation (Recommendation 17).

Retain the minimal fee for access to personal information (Recommendation 25).

Streamline the complaints process in the province's privacy laws

Align relevant provisions of the *Personal Information Protection Act* and *Freedom of Information and Protection of Privacy Act* in relation to the complaints process (Recommendation 26).

Strengthen the Information and Privacy Commissioner's oversight powers (Recommendations 27 and 29).

INTRODUCTION

The importance of protecting citizens' personal information was recognized by governments across Canada with the enactment of public-sector privacy laws. In British Columbia, the *Freedom of Information and Protection of Privacy Act* (FIPPA) came into force in 1993.

Before 2001, though, only one jurisdiction in Canada had a private-sector privacy law. In 1993, Québec enacted *An Act Respecting the Protection of Personal Information in the Private Sector*.

The federal private-sector privacy law, the *Personal Information Protection and Electronic Documents Act* (PIPEDA) came into force in three stages beginning in 2001 and regulates the way Canadian businesses collect, use and disclose personal information of their customers. The PIPEDA applies to all Canadian provinces unless a province has enacted a "substantially similar" privacy law — in which case the provincial law will regulate private-sector privacy for intra-provincial matters. To date, only British Columbia and Alberta have followed Québec's example and enacted such laws.

Anticipating the passage of the federal law, the Legislative Assembly of British Columbia appointed an all-party Special Committee on Information Privacy in the Private Sector on July 14, 1999, which submitted its report in March 2001. This Committee recommended, among other things, the enactment of information privacy legislation for BC's private sector and harmonization with similar laws.[1]

STATUTORY REVIEW PROCESSES

British Columbia's *Personal Information Protection Act* (S.B.C. 2003, c. 63) came into force on January 1, 2004. The Act includes a provision [s. 59] requiring a special committee of the Legislative Assembly to conduct a comprehensive review within three years of the in-force date and to submit its report to the House within one year after the date of its appointment. Subsequent reviews of the Act will take place at least once every six years, with the first six-year period beginning on the date of the submission of this report to the Legislative Assembly.

Accordingly, on April 19, 2007, the Legislative Assembly appointed an all-party Special Committee to Review the Personal Information Protection Act (the Committee) and instructed it to report back to the House within one year after the date of its appointment. Since parliamentary committees in British Columbia are appointed on a sessional basis, the Legislative Assembly reappointed the Committee on February 19, 2008, with renewed terms of reference. The Committee's review of the BC *Personal Information Protection Act* (PIPA) happened to coincide with similar statutory review processes at the national level and in Alberta.

With respect to the PIPEDA, the first scheduled review of the administration of Part 1 of the Act, Protection of Personal Information in the Private Sector, was conducted by the House of Commons Standing Committee on Access to Information, Privacy and Ethics (PIPEDA Review Committee). The PIPEDA Review Committee heard from 67 witnesses between November 20, 2006 and

[1] The Legislative Assembly of British Columbia, Special Committee on Information Privacy in the Private Sector, *Report*, 2001, pp. 9-10.

February 22, 2007, and received 34 submissions from additional individuals and organizations. It submitted its report in May 2007.[2]

The first review of Alberta's private-sector privacy law was undertaken by the Select Special Personal Information Protection Act Review Committee (Alberta PIPA Review Committee). This all-party parliamentary committee was appointed by the Legislative Assembly of Alberta on May 16, 2006 and submitted its report in November 2007. The Alberta PIPA Review Committee heard ten oral presentations from various organizations and individuals and received 65 written submissions.[3]

BC CONSULTATION PROCESS

The Committee held 11 meetings in total, which are listed in Appendix A. To begin its review, we received initial briefings from the Information and Privacy Commissioner (the Commissioner) for British Columbia (May 29 and November 7, 2007) and the Director of the Privacy and Legislation Branch, Ministry of Labour and Citizens' Services, which is responsible for the administration of the Act (May 16, 2007).

On the Committee's behalf, Mary Polak, MLA and the research analyst attended the 2007 PIPA Conference, organized by the offices of the Alberta and BC Information and Privacy Commissioners. This educational forum for businesses and non-profits was held in Vancouver from September 20 to 21, 2007. Research staff also participated in the Lancaster House Audio Conference: Enforcing Privacy Rights in the Workplace, which took place on November 1, 2007.

In terms of public consultation, call-for-submission ads were placed twice in the province's daily newspapers (November 17, 2007 and January 12, 2008). Invitations were also sent, via e-mail, to 130-plus organizations asking them to participate in the statutory review process.

By the deadline (February 29, 2008), the Committee had received 31 written submissions. Of these, the majority came from industry and professional associations, with the remainder from individuals. In addition, the Committee heard 12 presentations from organizations and individuals at public hearings held in Victoria (February 6, 2008) and Vancouver (February 22, 2008).

With the witnesses' consent, written materials were posted on the Committee's website, the first time this practice has been adopted by a BC parliamentary committee. A witness list is presented in Appendix B. At this juncture, the Committee would like to thank everyone who participated in the consultation process for their valuable input on the first four years of the Act's implementation.

During its final deliberations, the Committee invited the Commissioner and the ministry representative to address technical matters on the workings of the Act. These briefings took place on April 2 and 8, 2008 respectively.

---

[2] 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, May 2007, p. 1; cited in future footnotes as PIPEDA Review Committee Report.

[3] Legislative Assembly of Alberta, Select Special Personal Information Protection Act Review Committee, *Final Report*, November 2007, p. 4; cited in future footnotes as Alberta PIPA Review Committee Report.

Before moving to our conclusions and recommendations, which form the bulk of this report, we outline the key findings of our consultations and the principles guiding our decisions.

KEY FINDINGS

- At this stage of the Act's development, the PIPA seems to be working well overall, based on the feedback we received from the Commissioner, government, organizations covered by the Act and privacy advocates.
- During the course of our review, it also became apparent that the PIPA aligns well with the federal legislation, the PIPEDA, and the Alberta PIPA.
- While large corporations and not-for-profit organizations based in BC have a good grasp of the legislation, the public is not as aware of the purpose, rules and scope of the Act.

OPERATING PRINCIPLES

Our deliberations on the recommendations we would propose to the House were guided by two operating principles. First, we agreed that it was essential to maintain, if not strengthen, the protection of the personal information of British Columbians within the context of a global business environment and rapid technological change. From this standpoint, we considered carefully whether the existing Act is robust enough to provide adequate protection over the next six years until 2014, when the next statutory review is scheduled to take place.

Secondly, as far as practicable, we decided that any recommendations for legislative changes would take into account the proposals of the federal PIPEDA and Alberta PIPA Review Committees so as to facilitate further harmonization with other private-sector privacy laws in Canada. Legislators serving on these committees also strived for consistency in their recommendations so as to assist private-sector organizations operating in more than one jurisdiction.[4]

Within the BC context, we have also sought, where appropriate, to promote consistency between the private sector and the public-sector privacy laws. While our mandate precludes consideration of a uniform privacy protection act covering both sectors, we have recognized the need for consistency in legislative language in comparable provisions to assist members of the public and to facilitate the work of the Office of the Information and Privacy Commissioner for British Columbia.

The Committee used these principles to guide its deliberations on the report's content. In the course of reviewing the various requests for legislative changes, it became clear that a few submissions focused on topics related to the administration of the public-sector privacy law or to other provincial statutes, such as the *Residential Tenancy Act*. We discussed these topics with the Commissioner who informed us that his Office would be addressing privacy concerns that dovetail with other laws.

Our review focused on those submissions that fell within the scope of the Act. In the next sections of the report, we propose two types of recommendations first, substantive amendments to fill gaps in the PIPA and then other changes to streamline the Act's provisions.

[4] See PIPEDA Review Committee Report, p. 1 and Alberta PIPA Review Committee Report, p. 5.

ACCOUNTABILITY FOR CROSS-BORDER DATA FLOWS

Section 4(2) of the PIPA requires an organization to be responsible for personal information under its control, including personal information that is not in its custody. However, there is currently no provision in either the BC or Alberta privacy law stating that an organization's responsibility extends to information that has been transferred to a third party for processing or storage outside Canada. By contrast, under the PIPEDA, an organization is responsible for personal information in its possession or custody, "including information that has been transferred to a third party for processing."[5]

In their joint submission, the BC Freedom of Information and Privacy Association (BCFIPA) and the BC Civil Liberties Association (BCCLA) reported that both public- and private-sector organizations have told them that it is almost impossible to avoid sharing personal information with and, in some cases, contracting the management of information to companies subject to foreign laws with inferior privacy protection.

To mitigate the problems arising from disparate laws, the BCFIPA and the BCCLA made two "modest recommendations" for the Committee to consider. First, to strengthen an organization's accountability for personal information practices, they recommended the following amendment:

> *Recommendation 7*
>
> *That an amendment be added to PIPA explicitly stating*
>
> *(a) That organizations are responsible for the personal information in their custody or control, including information that has been transferred to a third party for processing;*
>
> *(b) That organizations shall use contractual or other means to ensure compliance with the Act and provide a comparable level of protection while the information is being processed by a third party, regardless of where the third party is located;*
>
> *(c) That a contractor is required to notify the organization of any subpoena, warrant, order, demand or request made by a foreign court or other foreign authority for the disclosure of personal information to which PIPA applies; and*
>
> *(d) That a contractor is required to notify the organization of any unauthorized disclosure of personal information under PIPA.*[6]

Next, the province's major privacy advocacy groups urged the Committee to consider adopting the first recommendation of the Alberta PIPA Review Committee:

> *1. That the Act be amended to require organizations to notify individuals when they will be transferring the individuals' personal information to a third-party service provider outside Canada.*[7]

The response of the Office of the Information and Privacy Commissioner (OIPC) for British Columbia to the privacy advocates' proposals was mixed. The Office supported the first two

[5] PIPEDA (2000, c. 5), Schedule 1, Clause 4.1.3.
[6] BCFIPA/BCCLA Joint Submission, p. 13.
[7] Alberta PIPA Review Committee Report, p. 7.

portions of their recommendation, 7(a) and (b), since these are consistent with its own proposals to strengthen accountability.

However, the Commissioner expressed the following reservations about 7(c) and (d):

> *…a provision such as that contemplated by FIPA/BCCLA recommendation 7(c) would put foreign third-party service providers to which personal information has been transferred with the choice of complying with the PIPA disclosure requirement and foreign law. The United States federal Foreign Intelligence Surveillance Act, for example, makes it a federal felony for an organization to disclose, with certain extremely limited exceptions, that a subpoena or court order for disclosure under FISA has been served on the organization….*
>
> *…questions arise as to how FIPA/BCCLA recommendation 7(d) will work once a British Columbia organization has learned of a foreign demand for disclosure. The recommendation would require the third-party service provider to notify the British Columbia organization of a demand. What then? The FIPA/BCCLA submission does not say.*
>
> *Would a notified British Columbia organization be required to demand immediate return of the personal information, to try to thwart the demand in advance of third-party compliance? Would this embroil the British Columbia organization in violation of foreign law, which may sometimes have extra-territorial effect? If the demand is complied with abroad, would the British Columbia organization, upon learning of this, be required to notify affected individuals, and if so, to what end? If the duty to notify were to someone other than the British Columbia organization, the minister responsible for PIPA, the OIPC or the Ministry of Attorney General, what then? What could they do about a demand that has been complied with? There may be meaningful answers to these questions, but I am not aware of them at this time.*[8]

Furthermore, the Commissioner's Office could not support the Alberta "notification-of-data-export" recommendation. Its position is that a legal obligation to notify would not advance the accountability principle and "be all but meaningless in our world of ubiquitous, ever-shifting cross-border data flows."[9]

Lawyers practicing in the area of privacy law also did not support express disclosure requirements for cross-border data flows (as has been recommended in Alberta) on the grounds that current obligations to safeguard information are sufficient. They pointed out that their position is consistent with the recommendation of the PIPEDA Review Committee and the federal government response.

With due respect to our counterparts who served on the Alberta PIPA Review Committee, the Committee does not think a notification-of-data-export rule is the appropriate remedy. From our perspective, what the average person is most concerned about is whether there are adequate safeguards in place when personal information leaves Canada for processing — in particular, who has access and control. This involves holding an organization responsible for the business practices of third-party contractors, regardless of where they are located.

---

[8] April 7, 2008 Memorandum from David Loukidelis, Information and Privacy Commissioner, p. 2.
[9] OIPC Submission, p. 21.

Consequently, we support strengthening accountability for cross-border data flows in the Act, along the lines recommended by the Commissioner and privacy advocacy groups to make the BC PIPA consistent with the PIPEDA. However, we are not prepared to endorse the privacy advocates' proposal to go further by holding third-party processors outside Canada accountable for business practices. Our concerns are that this could create an unwieldy regulatory regime — particularly for the many small businesses in the province — and be confusing for private-sector organizations operating in more than one jurisdiction.

Therefore, in the interests of enhancing accountability in the Act and facilitating further harmonization with the federal privacy law, we recommend that:

1. section 4 of PIPA be amended to expressly provide that:

(a) organizations are responsible for the personal information they transfer to a third party for processing or for providing services to or on behalf of the transferring organization; and

(b) organizations must use contractual or other means to ensure compliance with PIPA, or to provide a comparable level of protection, for personal information they transfer to a third party for processing or for providing services to or on behalf of the transferring organization.

MANDATORY NOTIFICATION OF PRIVACY BREACHES

Section 34 of the PIPA requires organizations to protect personal information. However, neither the BC or Alberta Acts nor the PIPEDA currently require a private-sector organization to notify affected individuals that the security of their personal information has been compromised.

The Committee received several submissions pressing the case for mandatory notification on the grounds that privacy breaches can have serious consequences for consumers. The proponents included a victim of identity theft, who thought there should be strict penalties for companies that do not notify customers that their personal information is at risk.

The major privacy advocacy groups in the province, the BCFIPA and BCCLA, were also in favour. They pointed out that since Industry Canada has accepted the PIPEDA Review Committee recommendation that organizations be required to disclose security breaches, only the manner of disclosure is now a subject of debate. They endorsed the approach put forward by the Canadian Internet Policy and Public Interest Clinic. In its submission to the PIPEDA Review Committee, the latter advocated adopting a data breach notification rule, modelled on the California law.[10]

On the other hand, neither the banking industry nor the insurance industry supported the idea of adding a mandatory privacy breach notification provision. Their representatives urged the Committee to give organizations of all sizes sufficient time to fully adopt the privacy breach guidance documents, prepared by the BC Commissioner's Office, rather than establish a specific duty in law.

A law firm also thought the existing guidelines were adequate, whereas a legislative mechanism would be burdensome for small organizations. Members of the FOI and Privacy Law Section of the Canadian Bar Association's BC Branch were divided on the issue, with some favouring mandatory reporting; others regarding it as unnecessary; and still others proposing the adoption of a pragmatic approach to the question.

The OIPC submission pointed out that in the past, the Commissioner's Office had also questioned the need for an express duty to notify individuals affected by a privacy breach. However, its position has changed since both the PIPEDA and Alberta PIPA Review Committees have recommended enactment of express notification duties. Therefore, in the interests of harmonization alone, the OIPC recommends that PIPA remain aligned with developments in these jurisdictions by including an express requirement to notify in carefully defined and controlled circumstances. Its submission, though, made clear that the Office "would oppose any amendment requiring it to decide in all cases when notification is required, to determine the particulars of notification or to carry out notification. The OIPC believes this is not an appropriate role for it to play and is deeply concerned about the resource implications it carries."[11]

During its deliberations, the Committee weighed carefully the advantages and disadvantages of incorporating mandatory notification of privacy breaches into the PIPA. We concluded that a

[10] Canadian Internet and Public Policy Interest Clinic, Submission to the House of Commons Standing Committee on Access to Information, Privacy and Ethics on the PIPEDA, November 28, 2006, p. 21.
[11] OIPC Submission, p. 12.

notification requirement would be desirable in specific situations, but not essential for all personal information that has been compromised in some way.

We believe individuals have a right to be notified when their sensitive financial information has gone missing so that they can take steps to protect themselves against the misuse of credit information or identity theft. The loss of confidential medical records as a result of a break-in at a doctor's office or careless disposal is another situation requiring follow-up action.

In addition, we support the case put forward by the Commissioner's Office and privacy advocates for consistency in breach notification provisions of Canadian private-sector privacy laws — particularly in regard to the questions of who should be notified, how a notification process should be enforced and whether a penalty should be imposed.

Accordingly, we examined first the relevant recommendations of the other statutory review committees — recommendations 23 to 25 (PIPEDA) and 3 and 4 (Alberta) — and then the OIPC proposal. After due consideration, the Committee opted to endorse the latter as the best option for our province at this time. We think the Commissioner's proposal is well thought out and covers all the bases, except penalties for failure to notify. The latter is a desirable omission, in our opinion, since enforcement of penalties would be burdensome for the Office. Therefore we recommend that:

2. the PIPA be amended to include an express duty for organizations to notify affected individuals of unauthorized disclosure or use of their personal information. To be effective and not over-broad, the amendment should address the following considerations:

- **(a) the kinds of personal information that must be involved before notice may be required, with personal information that is likely to create risks of financial loss or fraud and unauthorized disclosure of sensitive health information being key considerations;**
- **(b) who must be notified (affected individuals and the OIPC, with a possible added requirement to notify credit reporting agencies or law enforcement agencies in cases where financial loss is a risk);**
- **(c) how notice is to be given;**
- **(d) the timing of the giving of notice;**
- **(e) the general content of notices; and**
- **(f) authority for the Commissioner to order an organization to notify affected individuals of a privacy breach, on conditions the Commissioner may specify, where the organization has not given notice and the Commissioner considers that PIPA requires it.**

DEFINITIONS

The Committee received a few requests to add new definitions or amend certain ones listed in section 1 of the PIPA. Before reviewing these proposals, we would like to respond to an interesting question posed by a citizen who asked why privacy is not defined in the Act. On the face of it, it does strike us as rather odd that neither the PIPA nor the province's public-sector privacy law defines privacy. At the same time, we appreciate that the concept may be difficult to express in legislative language. As the Commissioner's Office points out, "[p]rivacy is certainly a rich concept with several dimensions. It includes the right to control access to your physical space, your body, your thoughts, your communications and your information."[12]

In the private-sector context, we think an argument can be made for defining privacy as "an individual's right to control access to their personal information". On reflection, though, we realize that adding a context-specific privacy definition to an Act that is now four years old may complicate its implementation and so the proposal is not a feasible one at this stage of the Act's development.

DESTRUCTION

At the Victoria hearing, the Committee heard a presentation by the National Association for Information Destruction (NAID)-Canada, a non-profit trade association representing 22 Canadian companies that specialize in secure information and document destruction. Its representatives pointed out that most identity theft is the "low-tech variety," with criminals sifting through dumpsters or recycling bins for personal information carelessly discarded by merchants. Since businesses are routinely failing to destroy personal information and often mistake recycling or tossing it in the trash for proper destruction, they suggested that government and the OIPC consider launching a public education campaign promoting safe information destruction.

With regard to the Act, NAID-Canada acknowledged that the BC PIPA is the first privacy law in Canada to recognise the importance of protecting personal information at the end of its life cycle. However, from its perspective, section 35(2) needs to be backed up by adding to Part 1 a technology-neutral definition of information destruction — "i.e., 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."[13]

The Commissioner's Office, though, did not support the amendment for the following reasons. "The OIPC is not persuaded such a definition is necessary and notes that NAID's proposed definition may be too narrow. The existing s. 35(2) requirement to destroy personal information is technology-neutral and can evolve as technologies of information destruction (and reconstitution) evolve."[14]

While we agree with NAID-Canada that the careless disposal of personal information is a serious problem, we share the Commissioner's reservations about adding a definition to the PIPA that could

[12] OIPC Submission, p. 2.
[13] NAID-Canada Submission, p. 3.
[14] OIPC Submission, p. 37.

be interpreted too narrowly and end up being out of step with constantly evolving technology. Accordingly, unlike the other statutory review committees,[15] we recommend that:

3. a definition of "destruction" not be added to the Act.

INVESTIGATION

A law firm raised a concern regarding the application of the definition of "investigation". It suggested amending the definition to make it clear that the initial information that is discovered and leads to an investigation being carried out where there are reasonable grounds to do so, can also be considered as part of the collection of personal information for the purposes of the investigation. From the lawyers' perspective, not including that first piece of information creates a gap which is "not reasonable" — e.g., an employee's first offence noted on a video tape may not be admissible.

However, the Committee is reluctant to recommend any change in the wording of "investigation" for two reasons. First of all, we are not persuaded that the law firm's concern about the application of the definition warrants a legislative amendment. Secondly, the Canadian Bankers Association informed us that during the PIPEDA review process, the chartered banks had pressed for the adoption of the BC Act's definition of "investigation", which includes the prevention of fraud. In response, and in the interests of harmonization, the PIPEDA Review Committee proposed that the approach taken by the BC and Alberta private-sector laws in regard to investigations be followed.[16]

Therefore to avoid creating confusion and inconsistency, we recommend that:

4. no amendment be made to the current definition of "investigation" in section 1.

WORK PRODUCT INFORMATION

Finally, the Committee was asked to consider clarifying the meaning of "work product information" in the Act. After pointing out that the existing definition has brought clarity and certainty to businesses, the Insurance Bureau of Canada (IBC) recommended a minor amendment to the definition. It suggested that rather than "information prepared or collected" by an individual or group of individuals during the discharge of their employment duties, a better choice of words would be "information prepared or compiled" to more accurately reflect how work product information is generated in the insurance industry.[17]

While not regarding this as a pressing concern, the Commissioner's Office did not object to the Insurance Bureau's suggestion. However, it proposed that if the Committee recommended any change, it should be to add "compiled" to the existing list, not to substitute it for "collected".[18]

The Committee notes that the existing definition in the BC PIPA has been recommended by the PIPEDA Review Committee as a model for a definition of "work product" in the federal Act.

---

[15] Recommendation 3, PIPEDA Review Committee Report, p. 10; Recommendation 29, Alberta PIPA Review Committee Report, p. 32.
[16] PIPEDA Review Committee Report, p. 15.
[17] IBC Submission, p. 6.
[18] OIPC Submission, p. 31.

Nevertheless, we do not believe our acceptance of the sensible minor change in wording will have any effect on the consistency principle. Accordingly, we recommend that:

5. the definition of "work product information" in section 1 be amended by adding "or compiled" to the clause "information prepared or collected".

ORGANIZATION'S PRIVACY POLICIES AND PRACTICES

The BC Freedom of Information and Privacy Association and the BC Civil Liberties Association presented the case for more openness in organizations' privacy policies and practices, claiming that the lack of rigor in notification requirements (sections 5 and 10) is having an adverse impact on the implicit consent provision (section 8). Their recommendation was designed to clarify and strengthen the Act's wording so that it at least matches the standards of the openness principle incorporated in the PIPEDA:

> *Recommendation 2:*
>
> *a) That the "Openness Principles" of the Model Code for the Protection of Personal Information be incorporated more effectively into PIPA. The openness principle requires that an organization's privacy policy, practices and complaint process be clear, comprehensive and easily accessible.*
>
> *b) That, on or before collecting personal information from an individual, an organization should be required to provide the individual with or refer them to the organization's written privacy policy.*
>
> *c) That all the purposes, uses and disclosures of personal information intended by the organization should be made public as part of the "Required notification for collection of personal information".*[19]

However, the OIPC submission pointed out that in Order P06-04, the Commissioner held that section 5(c) of the PIPA does not require an organization to make a written privacy policy publicly available or available to an individual on request. Also, a statutory duty to make written privacy policies publicly available might have a significant impact on many small businesses and volunteer community organizations. Therefore, the Office "is, on balance, not sure that a broad, or unqualified, duty to make them publicly available in writing is desirable."[20]

In view of the Commissioner's ruling on the openness question and his Office's concern about the impact on smaller organizations, the Committee is reluctant to recommend any change. We think imposing a requirement may be particularly burdensome for very small businesses, where transactions with customers are more on a one-time basis and where the information is not routinely kept. Further, we recognize that many of the larger corporations and not-for-profit organizations have already developed written privacy policies and made them publicly available in order to provide assurance to their customers or clients that their sensitive and confidential information is being protected. Therefore we recommend that:

6. no amendment be made to the Act requiring an organization to make written privacy policies publicly available.

[19] BCFIPA/BCCLA Joint Submission, p. 9.
[20] OIPC Submission, p. 20.

CONSENT PROVISIONS

Like the other private-sector privacy laws in Canada, the BC PIPA is a consent-based statute. Consistent with international fair information principles, PIPA rules require an organization to obtain an individual's consent for the collection, use and disclosure of personal information, and to collect only as much information as is necessary for the stated purposes.

Most of the feedback the Committee received from witnesses indicated that the consent provisions in Part 3 of the Act are working well and so at this stage of the Act's development, we are reluctant to recommend any major changes to these core provisions. This is a decision we made after considering a request from the province's privacy advocacy groups to revisit the concept of implicit consent. On this matter, we believe that the existing provision [s. 8] currently recognizes the importance of giving people a personal choice, or a certain level of responsibility, with respect to handling their own personal information. Therefore, in our opinion, the existing "opt-out" option is a desirable approach to take. Also, we do not want to be overly prescriptive with core concepts like implicit consent, which are up to the Commissioner and, ultimately, the courts to interpret.

The Committee considered three other issues related to the consent provisions in Part 3 of the Act. These topics — identity verification, credit card receipt safety and blanket consent forms — are not discussed separately in the reports of the federal and Alberta statutory review committees.

IDENTITY VERIFICATION

Section 7(2) of the Act specifies that an organization supplying a product or service must not require an individual to consent to the collection, use and disclosure of personal information beyond what is necessary to provide the product or service.

The Committee received a few complaints about some businesses collecting too much personal information. For example, a Vancouver chartered accountant asked why a bank teller needed to make copies after seeing his ID; why a notary wanted to copy his passport and driver's licence; and why an e-mail sent by a bank confirming the terms of a certificate-of-deposit account contained his name, residential address and phone number – for the whole world to see! A lawyer who does conveyancing also expressed concern about the amount of information requested by out-of-province lenders for identity verification.

In some cases, the remedies proposed by individual citizens focused on the need for more education and training. For example, one concerned consumer suggested offering a basic course on privacy requirements to new and existing companies, and another course on privacy rights to individuals. Also, a parent, who is concerned about the practice of disclosing her daughter's name in e-mails related to her school and leisure activities, proposed that organizations in both the public and private sectors need a refresher course on implementing privacy laws.

During its deliberations, the Committee realized that individual complaints about banks and law firms were not isolated incidents but symptomatic of a widespread business practice in the financial services sector and the legal profession. We considered whether the Act needs "more teeth" to discourage organizations from being over-zealous in collecting or replicating personal information.

We decided not to recommend any changes to the core consent provisions for the following reason. Since the Act has been in force for only four-plus years, the Commissioner's Office has not had a lot of opportunity yet to formally interpret and issue decisions regarding the application of section 7(2). To date, we understand that the Office has tried to hold organizations to "a pretty high standard" and intends to continue to be active in promoting best practices in information collection.

Instead, we opted to strengthen section 11, Limitations on collection of personal information, in line with the PIPA rule requiring an organization to collect only as much personal information as is necessary for the stated purposes. Accordingly, we recommend that:

7. section 11 be amended by adding "and necessary" at the end of the clause "a reasonable person would consider appropriate".

In addition, while we support the Commissioner's efforts to date, we think more can be done by his Office to make smaller private-sector organizations aware of the requirement to collect only the information they need to conduct business with their customers or clients. Since very small businesses are not in a position to hire privacy consultants or to attend training sessions on privacy law compliance — or are even conscious of their obligations under the Act, for that matter — we recommend providing educational information via the OIPC website as the best option to pursue.

8. the Office of the Information and Privacy Commissioner consider developing an on-line resource guide, using the FAQ format, to educate private-sector organizations about the topic of information collection.

SAFETY OF CREDIT CARD RECEIPTS

At the Vancouver hearing, the Committee heard from the owner of an identity theft prevention company who was concerned about the lack of consideration in the Act for the way an organization may misuse personal information on the printed copy a credit cardholder signs at the point of sale. He described the current practice of processing this information, conducted mostly by restaurants, entertainment, hospitality and other service industries, as "private data suicide" and proposed truncating or eliminating the number as a remedy.

The witness suggested adding the following paragraph to section 8, Implicit consent:

> *(5) A purchaser, when conducting business with a credit card, provides consent to the organization to use the information on the card in order to process the business transaction. The consent does not include posting the full 16 digits of the credit card number, the expiration date, their printed name and signature on the receipt to be left for anyone to access.*

The Committee considered whether a legislative change was really necessary in light of the fact that increasingly, businesses operating in BC are now using point-of-sale machines that include only the last four digits of a customer's credit card number and omit the expiration date. A prime reason for this new practice is that the truncation of credit card (and debit card) numbers on receipts printed electronically is now mandatory in the US, under s. 605(g) of the federal *Fair Credit Reporting Act*.

However, we anticipate that some small businesses in BC — particularly, mom-and pop operations and cab companies — will continue, at least for the foreseeable future, to record a credit card number by making an imprint or copy of the card. One option we considered to enhance the safety of a receipt, not printed electronically, is some form of identity tag for the person who accepts the credit card. That way, a customer could trace the information associated with a sale or business transaction. Then, if the credit information is sold or stolen for financial fraud purposes, the business owner or employee processing the credit card payment could be held accountable.

On reflection, the Committee realizes that an ID tag is not a very practical idea. Nonetheless, we think some kind of action is needed to remind businesses to be more careful with the sensitive personal information they are handling in credit card and debit card transactions. We believe prevention of theft of personal information has to be an important policy goal as the cost to society in general and government in particular of having to investigate fraud cases is considerable, quite apart from the devastating impact on the victims of ID theft. Therefore we recommend that:

9. the Office of the Information and Privacy Commissioner consider using its website as the medium to encourage small business owners to use safer methods for processing credit and debit card transactions and to raise public awareness about the risks of discarding receipts.

USE OF BLANKET CONSENT FORMS

At the Victoria hearing, the Insurance Brokers Association of BC (IBABC) informed the Committee that the verbal-consent rule and the PIPA provisions relating to implicit consent [s. 8(2)] and the collection of personal information without consent [s. 12(2)] were working well. However, IBABC-member brokers were "extremely concerned" about the use of blanket consent forms by banks that own an insurance subsidiary.

The IBABC representative explained that the federal *Bank Act* and the provincial *Financial Institutions Act* both provide for insurance as a financial pillar that is separate and distinct from other banking functions. In real terms, these statutes dictate that:

- Insurance can only be sold, and insurance advice can only be given, by qualified, licensed personnel.
- Banks can own an insurance subsidiary, but are prohibited from retailing insurance from their branches.
- The business office of the insurance agent must be located in premises that are separate and distinct from the business office of a savings institution.

In the brokers' view, the language used in the blanket consent forms that grants the banks permission to share personal information across the banking and insurance pillars is contrary to the intent of these two statutes. Their other concern is that the forms can be used to gain permission to use credit information in ways that the consumers may not be aware of, and if made fully aware, would not agree to.

The IBABC urged the Committee to include a clause in the PIPA that prohibits blanket consent across financial pillars, and to review the relevant sections of the Act in conjunction with Part 6 (Credit Reporting) of the *Business Practices and Consumer Protection Act.* Part 6 provides for sharing of credit information as long as the individual gives permission, and it requires organizations using the information to disclose the reasons for adverse actions (such as denial of sale or increase of cost) that result from use of the information.

The Committee was receptive to the brokers' request partly out of sympathy for the customer who applies for a bank loan, or has a department store account, and then receives numerous unsolicited offers to buy life or health or travel insurance. Also, from our perspective, the use of blanket consent forms is at odds with the principle of informed consent that forms the basis of private-sector privacy legislation. In our view, informed consent means more than a one-time blanket signature on a consent form couched in general language. To strengthen this important principle in the BC PIPA, in terms of its application to provincially regulated financial institutions, we recommend that:

10. the Act be amended to include a clause that prohibits blanket consent across financial pillars, and be reviewed for consistency with credit-reporting requirements in Part 6 of the *Business Practices and Consumer Protection Act.*

EXCEPTIONS TO CONSENT

The PIPA requires an organization to obtain consent from an individual in order to collect, use or disclose her or his personal information, unless an exception to consent applies.

Some submissions claimed that the consent exceptions relating to investigations or legal proceedings are too narrow, while others focused on broadening exceptions to disclosure. Regarding the former, the relevant provisions of the PIPA are sections 12(1)(c), 15(1)(c) and 18(1)(c) that permit the collection, use and disclosure of personal information without consent where it is reasonable to expect that the collection with consent would compromise the availability or the accuracy of the personal information, and where the collection, use and disclosure is reasonable for the purpose of an investigation or a proceeding.

WITNESS STATEMENTS

The most complex request related to investigations/proceedings came from the Insurance Bureau of Canada (IBC), the national trade association of general insurers. First, the IBC submission suggested that the Act's "very broad" definition of personal information does not address an issue faced every day by property and casualty (P&C) insurers in the course of obtaining witness statements from people who saw the incident or who have information that is necessary for the investigation of the claim. Next, the IBC was opposed to the view that an insurer should obtain the consent of the claimant or potential claimant before obtaining witness statements. Finally, the IBC sought to protect insurers' ability to investigate and settle a claim when an access request is received, arguing that disclosure may harm their handling of a claim and any resulting litigation.

To clarify these three interrelated issues, the IBC recommended the following amendments:

> 1. *The definition of "personal information" should be amended to clarify that personal information expressed by one individual ("the witness") about another ("the subject") is the personal information of the witness.*
>
> 2. *As well, sections 12, 15 and 18 of the PIPA should be amended to provide that an organization may, during the course of investigating and settling contractual issues or claims for loss of damages, collect, use and disclose a witness statement without the subject's knowledge or consent.*
>
> 3. *Re the exemptions in section 23(3) of the PIPA for denying an access request, "IBC recommends the following amendments:*
>   - *i) amend section 23(3)(a) to include specific reference to "litigation privilege",*
>   - *ii) add a new exemption in section 23 as follows: "23(3)(g) the information was generated in the course of the process to investigate and settle contractual issues or claims for loss or damages."*
>   - *iii) add clarification in PIPA that when litigation has commenced, the provincial rules of civil procedure should govern and prevail over access provisions in PIPA."*[21]

[21] IBC Submission, p. 4.

However, the Office of the Information and Privacy Commissioner (OIPC) initially opposed these amendments for the following reasons. It pointed out that the first recommendation runs counter to one of the Act's main purposes, and features — namely, "that it gives individuals a right of access to their own personal information in the custody or under the control of an organization. This is an internationally-recognized principle and is a key part of any modern privacy law."[22]

Regarding the second recommendation, the OIPC expressed its position in the following way:

> *There is no reason why consent could not be built into the contract of insurance. The insured would consent, through the terms of the insurance policy, to the insurer collecting personal information in the form of statements by witnesses to an accident or other events giving rise to an insurance claim by the insured. If the insured later tried to revoke that consent, as s. 9(1) of PIPA permits, the insurer could invoke policy terms denying coverage.*
>
> *Further, in cases where the insurer has grounds to believe that the insured is making a false claim or otherwise has breached the insurance policy, or any law, ss. 12, 15 and 18 of PIPA authorize the insurer to collect, use and disclose personal information without consent where it is reasonable to expect that obtaining consent "would compromise an investigation or proceeding" and the collection, use or disclosure "is reasonable for purposes related to an investigation or a proceeding."*[23]

Finally, the Commissioner's Office rejected the IBC amendments to broaden exemptions in section 23(3) on the grounds that there should be no new barriers to individuals' access, and that the IBC has not made the case for the need for such sweeping changes, which have not been recommended by the other statutory review committees.[24]

In fact, in response to the same request from the IBC, the PIPEDA Review Committee concluded, as follows:

> *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.*

[22] OIPC Submission, p. 26.
[23] OIPC Submission, p. 25.
[24] OIPC Submission, pp. 27-28.

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.[25]

In response to the PIPEDA Review Committee's report, Industry Canada sought public input on the issue of witness statements, as well as other topics. Its report on the outcome is still pending.

The Committee has learned that since our consultation process ended on February 29, 2008, follow-up discussions have occurred between the BC Commissioner and the IBC on the problematic issue of witness statements.[26] As a result, the Commissioner now suggests that the Insurance Bureau's concerns could be addressed by amendments to the PIPA's substantive provisions [ss. 12, 15, 18] governing non-consensual collection, use and disclosure of personal information.[27]

The Committee supports the Commissioner's suggestion because it will assist not only the insurance industry but also Privacy Commissioners across Canada come to a resolution of this complex issue. Since section 33.1 of the FIPPA has already been amended to enable ICBC to conduct its business, we also think it is important to recognize the specialized nature of the insurance business in the private-sector privacy law. Accordingly, we recommend that:

11. the Act be amended by adding a clause to ss. 12, 15 and 18 to allow the collection, use and disclosure without consent of personal information necessary for the insurer to assess, adjust, settle or litigate a claim under an insurance policy.

SELF-REGULATORY ORGANIZATIONS

The Committee received another request to broaden the scope of the consent exception for an investigation from the Mutual Fund Dealers Association (MFDA) of Canada, the national self-regulatory organization (SRO) for the distribution side of the mutual fund industry. Its submission indicated that mutual fund dealers are having difficulty obtaining access to the personal information necessary for the performance of effective investigations due to the current wording of section 18(1)(j). This subsection confines disclosure without the consent of the individual to an offence under the laws of Canada or a province. This poses practical difficulties for the MFDA, since its activities are generally in the nature of enforcement of regulatory standards. Further, the BC

[25] PIPEDA Review Committee Report, p. 21.
[26] IBC E-mail Communication to PIPA Committee, March 28, 2008.
[27] April 7, 2008 Memorandum from David Loukidelis, Information and Privacy Commissioner, p. 3.

Securities Commission (BCSC) can invoke this section for breaches of the BC *Securities Act*, but MFDA cannot apply it for breaches of its rules, despite being recognized as an SRO by the BCSC.

To remedy this situation, the MFDA made two suggestions:

> *The proposed amendment is*
> *18(1)(j) the disclosure is to a public body, a law enforcement agency or regulatory organization in Canada, concerning an offence under the laws of Canada, or a province or the by-laws, rules, regulations or policies of a self-regulatory organization recognized by the British Columbia Securities Commission, to assist in an investigation, or in the making of a decision to undertake an investigation,*
> *(i) to determine whether the offence has taken place, or*
> *(ii) to prepare for the laying of a charge, or the commencement or prosecution of proceedings [strike out "or the prosecution of"] in respect of the offence,*
>
> *An alternative suggestion is to modify section 18(1)(j) to include the by-laws and rules of prescribed regulatory organizations in addition to the laws of Canada or a province. This would provide the government with a certain degree of flexibility in determining which regulatory organizations' by-laws and rules should be included in the exception set forth in 18(1)(j).*[28]

The Commissioner, though, questioned whether it is necessary to make the change solely for the purposes of the MFDA, since the definition of "investigation" in the PIPA already refers to an investigation respecting the improper trading of a security by an organization represented by the BCSC. He suggested that it may be better for the Committee to refer to a regulatory organization prescribed in regulations under PIPA to offer flexibility in designation of SROs.

The Committee paid particular attention to this request because we think it is important to support efforts that will facilitate investigations into potential wrongdoing. On further inquiry, we received different opinions from the Commissioner and government on the question of whether it is appropriate to establish a separate regulatory scheme under the PIPA for national SROs operating in British Columbia. Pending a resolution of this matter by the parties involved, we recommend that:

12. no amendment be made to section 18(1)(j) of the Act.

RISK MANAGEMENT SERVICES

Another request for a consent exception came from the Canadian Medical Protective Association (CMPA). The CMPA is a mutual defence organization run by physicians and the main provider of medical-legal assistance to Canadian doctors, including some 10,000 physicians in BC. It asked the Committee to consider exempting its members from the requirement to obtain a patient's express consent before sharing personal health information with the association's risk management advisers.

The submission stated that it is "extremely important" in private-sector privacy legislation to have clear exceptions that permit physicians to communicate with the CPMA about medical-legal issues

[28] MFDA Submission, p. 3.

with respect to both day-to-day practice and existing or anticipated legal proceedings. Accordingly, the CMPA proposed two changes, summarized as follows:

> 1. *The CMPA recommends adding a new subsection (q) to section 18(1) of the BC PIPA to specifically authorize the disclosure of personal information about an individual without consent if "**the disclosure is to the organization's insurer or professional liability provider for the purpose of obtaining error [reduction] or risk management services."***[29]
>
> 2. *In order to ensure that organizations are not unnecessarily restricted in the disclosure of personal information for the purpose of proceedings that are either contemplated or have been commenced, the CPMA suggests that the definition of "proceeding" in section 1 be slightly amended to specifically include "anticipated proceedings", and that amendments be also made to sections 18(1)(c) and 15(1)(c) to permit non-consensual use or disclosure without references to "with the consent of the individual would compromise an investigation or a proceeding".*[30]

The Commissioner's Office, though, did not support the first recommendation. Its submission pointed out that a physician has the option now of notifying patients and obtaining their consent to disclosure of personal information necessary to obtain CMPA error reduction and risk management services. Also, the reports of the other statutory review committees have not included recommendations in this area. Further, the CMPA has not offered evidence of any pressing problem with PIPA's current language.

Regarding the second recommendation, the Office does not object to amendment of the term "proceeding" to include proceedings in "reasonable contemplation" (not "anticipated" proceedings, as the CMPA suggests), but it does not endorse the other changes:

> *The OIPC does have concerns about the CMPA's proposed ss. 15(1)(c) and 18(1)(c) amendments. At present, these provisions authorize, respectively, non-consensual use and disclosure of personal information where "it is reasonable to expect" that use or disclosure "with the consent of the individual would compromise an investigation or proceeding" and the use or disclosure "is reasonable for purposes related to an investigation or a proceeding". The CMPA would eliminate the requirement that obtaining consent could reasonably be expected to compromise the investigation or proceeding.*
>
> *The consent of individuals to the collection, use and disclosure of their personal information is at the core of PIPA and any departure from that default principle should proceed only where it is shown to be clearly necessary to address a pressing objective or concern. The CMPA has not shown that the present test of compromise of an investigation or proceeding has impeded efficient and effective investigation and defence of claims by the CMPA or others. The OIPC acknowledges that the provisions of Alberta PIPA comparable to ss. 15(1)(c) and 18(1)(c) are very similar to the CMPA's proposal, but the OIPC does not believe that the harm test in our PIPA should be eliminated.*[31]

[29] CMPA Submission, p. 4.
[30] CMPA Submission, p. 5.
[31] OIPC Submission, p. 34.

The Committee supports the position of the Commissioner's Office and recommends that:

13. "a reasonably contemplated" proceeding be added to the definition of "proceeding" in section 1 of the Act.

14. no amendments be made to the consent exceptions in sections 15(1)(c) and 18(1)(c) of the Act.

PUBLICLY AVAILABLE INFORMATION

Some members of the BC Branch of the Canadian Bar Association (CBA) think the consent exceptions in the PIPA for the collection, use and disclosure of personal information available to the public are too broad [ss. 12(1)(e), 15(1)(e) and 18(1)(e)]. They sought to narrow these exceptions for the following reasons:

> *Specifically, as currently drafted the provisions provide, in effect, that once information becomes publicly available from a prescribed source, such information may be collected, used and disclosed for any and all purposes without limitation. This is of particular concern as technological advances have not only increased the scope of public disclosures of large amounts of information but also the ability of private-sector organizations to use technology for the wholesale copying and 'mining' of such information.*[32]

To bring such exceptions in line with the PIPEDA provisions, the lawyers suggested that the "publicly available" provision in the PIPA be limited to the collection, use and disclosure without consent only for the purposes for which the information was published. However, other CBA members felt the proposed amendment would result in an unnecessarily narrow interpretation of the provision.

The Committee is not persuaded by the argument that consent exceptions need to be narrowed for personal information that is already available in the public domain. Therefore we recommend that:

15. no amendments be made to the consent exceptions in sections 12(1)(e), 15(1)(e) and 18(1)(e) of the Act.

BUSINESS TRANSACTIONS

The Committee considered another request from privacy lawyers regarding section 20 of the PIPA that permits certain non-consensual disclosure and use of personal information about "employees, customers, directors, officers or shareholders" of an organization in the context of a business transaction. The submission of the BC Branch of the Canadian Bar Association presented the case for broadening this consent exception in the following way:

> *Although section 20 has generally worked well, the exception currently is limited to personal information about "employees, customers, directors, officers or shareholders" of the organization. It has been suggested that limiting the exception to these classes of information is arbitrary and does not reflect the intention of the provision, which is to*

[32] CBABC Submission, p. 3.

> *allow organizations to disclose personal information that is reasonably necessary to proceed with the business transaction, subject to the protections stipulated in the section. This may include information about other classes of individuals such as candidates for employment, employees of other organizations with which the disclosing organization conducts business. Accordingly, some members have suggested that the exception be expanded to cover all personal information under the custody or control of the organization that is reasonably required to be disclosed in conjunction with the business transaction.*[33]

In response, the Commissioner's Office acknowledged the concern that the existing categories of personal information, being limited to "employees, customers, directors, officers and shareholders", may be unduly restrictive such that section 20 does not fully implement the legislative intention underlying the provision. To address this concern, the Office recommended an amendment to section 20 of the PIPA.[34]

To facilitate the transfer of personal information in the sale of an organization or its business assets, the Committee recommends that:

16. section 20 of the Act be amended to provide that an organization may disclose or collect, without consent, personal information in its custody or under its control (including personal information about its employees, customers, directors, officers or shareholders) that is reasonably required to be disclosed or collected in conjunction with a business transaction.

HEALTH RESEARCH

At the Vancouver hearing, the British Columbia Cancer Agency (BCCA) urged the Committee to revisit the consent exception in section 21(1)(b), which does not permit an organization to disclose personal information if the information will be used to contact persons to ask them to participate in the research. The BCCA representative pointed out that at present, section 35(a.1) of the *Freedom of Information and Protection of Privacy Act* (FIPPA), also prohibits disclosure of information from public databases for research contact purposes. As a result, this section has had the unanticipated effect of preventing or holding up key health research in the public interest, including studies of vaccination coverage, causes of cancer and Parkinson's disease.

On behalf of the BCCA and the BC Cancer Research Centre, the witness asked the Committee to consider modification of section 21(1)(b) in anticipation that this section is likely to have similar unanticipated adverse effects on the common good in the near future, as health research and care in BC increasingly involves information from organizations in the private sector and the public sector. To illustrate how section 21(1)(b) might prove counterproductive, the witness cited the example of prostate cancer screening carried out by private labs such as LifeLabs and BC Biotech. If the BCCA were to elect to proceed with a provincial program of screening by continuing to rely on private labs for initial blood testing, these firms would be unable to disclose names of those tested to the BCCA

[33] CBABC Submission, p. 3.

[34] Recommendation 6, OIPC Submission, p. 22.

due to s. 21(1)(b). This would make it impossible to fully evaluate the effectiveness of the provincial program, unless the Act is amended to permit disclosure of contact information for health research.

The submission of the Office of the Information and Privacy Commissioner (OIPC) expressed similar views about the impact of existing disclosure rules:

> *The Commissioner is on record as having been opposed to enactment of s. 35(a.1) and has the same concerns respecting s. 21(1)(b). The OIPC recognizes that there is a need to protect privacy in relation to respecting disclosure of patients' personal information for the purpose of asking them to participate in research. The OIPC continues to be concerned, consistent with the Commissioner's statements in recent years, that these provisions in PIPA and FIPPA inappropriately impede research and should be replaced with a more balanced approach.*[35]

On further inquiry, the Committee learned that the Commissioner would support a provision that allows the use of information for contact purposes, under controlled circumstances. This would have to address situations where, for example, the contact itself could reveal a patient's disease status to family members — for example, stigmatized conditions such as HIV/AIDS could be disclosed by the mere fact of an envelope arriving at the family home with a return address showing it is from a health authority or a researcher.

To minimize such privacy risks, the Commissioner favours physicians making the contact on behalf of researchers. His Office could approve the use of personal health information for this purpose according to criteria that it devises — based on the Canadian Institute for Health Research best-practice guidance — or else generally set out in legislation.

The Committee believes that in certain circumstances, the greater good of society outweighs the individual's need for privacy protection. In our opinion, this request for access to personal health information is a case where the public good unquestionably trumps a minor infringement on privacy — namely, the disclosure of contact information for the purpose of conducting clinical trials. Some committee members, though, are not convinced that a research ethics board has the necessary expertise with respect to privacy risks.

To accommodate their concern, the Committee prefers the option of the OIPC approving the criteria, along the lines of the consequential amendment to FIPPA's s. 35a.1, proposed in Bill 24, E-Health (Personal Health Information Access and Protection of Privacy) Act — which was introduced in the Legislative Assembly on April 10, 2008. Therefore to facilitate consistency with the province's public-sector privacy law, we recommend that:

17. section 21(1)(b) of the PIPA be repealed and replaced with a provision stating that personal information can only be disclosed for research contact purposes with the approval of the Commissioner according to criteria set out in the Act or by regulation.

[35] OIPC Submission, p. 38.

ARCHIVAL OR HISTORICAL RESEARCH

The Committee also received a submission from a citizen involved in genealogy who is finding it increasingly difficult to obtain information about births, marriages and deaths of BC residents. In his opinion, it is unreasonable and carrying privacy too far to restrict details about a birth in British Columbia for up to 120 years, and he asked the Committee to consider changing privacy legislation.

During its deliberations, the Committee established that provisions in both the PIPA [ss. 22(c),(d)] and the FIPPA [ss. 36(c),(d)] permit non-consensual disclosure of personal information for archival or historical purposes if the information is about someone who has been dead for 20 or more years, or if the information is in a record that has been in existence for 100 or more years. We also consulted the 2004 FIPPA Review Committee Report, which reached the following conclusion:

> *[T]he Committee concluded that the existing cut-off date is a reasonable minimum limit and strikes the right balance between not making archivists and family-oriented researchers wait too long and protecting the personal information of centenarians who are still alive…. While we are not proposing any change to section 36(d) at this time, we would ask future statutory review committees to keep a watching brief on this topic, given the anticipated increase in longevity.*[36]

The Committee considered carefully the question of what harm would be done by relaxing the 100-year rule and permitting both public- and private-sector organizations, such as churches, to release what some might regard as relatively innocuous information earlier. On balance, though, we were persuaded by the argument of our colleagues on the 2004 FIPPA Review Committee that citizens of whatever age expect their personal information to be protected under the Act. Accordingly, in the interests of protecting personal privacy and maintaining consistency with the public-sector privacy law, we recommend that:

18. no amendment be made to section 22(c) or 22(d) of the Act at this time.

EMPLOYEE PERSONAL INFORMATION

The final request for a consent exception the Committee considered came from the Office of the Information and Privacy Commissioner (OIPC). It presented the case for amending the Act in relation to "employee personal information", as follows:

> *Under PIPA, "employee personal information" is personal information that is reasonably required to establish, manage or terminate a work relationship. It does not include personal information about employees held by an organization that is not related to those things. Employee personal information is a distinct category of personal information and PIPA has special rules for collection, use and disclosure of "employee personal information" [ss.13, 16 and 19].*

[36] The Legislative Assembly of British Columbia, Special Committee to Review the Freedom of Information and Protection of Privacy Act, Report, *Enhancing the Province's Public Sector Access and Privacy Law*, May 2004, pp. 26-27.

PIPA's rules about "employee personal information" do not apply to former employees. To give only one example, the way PIPA now reads, where an employer needs to disclose personal information of former employees to pay them post-employment benefits such as pensions, the employer would have to obtain the consent of the former employees. The OIPC doubts this was intended by the Legislature and recommends an amendment to permit non-consensual use and disclosure of "employee personal information" after termination of the employment relationship. The amendment would have to be carefully tailored, however, to limit it to situations where the use or disclosure is necessary to manage post-employment relations or dealings between the employer and former employee. The OIPC notes that the Alberta legislative review committee made such a recommendation (Recommendation 18).[37]

The Committee supports the Office's sensible request and recommends that:

19. the PIPA be amended to permit non-consensual use and disclosure of "employee personal information" after termination of the employment relationship where the use or disclosure is necessary to manage post-employment relations or dealings between the employer and former employee.

[37] OIPC Submission, p. 16.

ACCESS-RELATED TOPICS

Part 7 of the PIPA covers access to and correction of personal information. Under the rules of the Act, an organization is required to ensure personal information is accurate for the purposes for which it is collected; and upon request, provide individuals with access to their own personal information.

ACCESS TO PERSONAL INFORMATION

Section 23 of the PIPA permits individuals to make an access request to an organization for their own personal information and allows an organization to withhold certain information.

The Insurance Bureau of Canada (IBC) sought clarification on whether access to personal information referred to the information itself, or to the documents that contain the information. It recommended that the Act be amended to provide organizations with an option of how they provide access to personal information in order to eliminate the inefficiency of the current approach of copying all documents.[38]

However, the Office of the Information and Privacy Commissioner (OIPC) opposes this recommendation for the following reasons:

> *First, PIPA is not "unclear" on this point. It is clear beyond doubt that the right of access under PIPA is a right of access to personal information and not to a summary of personal information. Under s. 23(1) of PIPA, an organization must provide an individual who requests it with "the individual's personal information under the control of the organization". There is no ambiguity here. Section 23(1) clearly requires an organization to provide access to the "individual's personal information", subject to any severing under s. 23, not access to a summary.*
>
> *In any event, the suggestion that organizations should be given the option, in their sole discretion, of refusing access to personal information and providing some sort of summary—the IBC does not suggest any criteria to govern this proposed new authority, which would be open to abuse—runs counter to PIPA's purposes. As noted above, an individual's right of access to her or his own personal information is a key component of any respectable privacy law because that right empowers individuals to monitor for themselves an organization's compliance with PIPA. The crucial right of access could be rendered meaningless by a new right for an organization to summarize personal information, not provide access.*
>
> *The OIPC notes that nothing in PIPA prevents insurers from offering their customers summaries of insurance claims files—these are the kinds of files the IBC has said are problematic—on an optional basis. If an insurer were to offer claims file summaries as an option, they might prefer that. As long as the insurer did not ignore an access request made under PIPA, this alternative arrangement would be acceptable and could improve customer relations.*[39]

[38] IBC Submission, p. 6.

[39] OIPC Submission, pp. 29-30.

The Committee considered carefully the Insurance Bureau of Canada's request but agrees with the Commissioner's interpretation of section 23. Therefore we recommend that:

20. no amendment be made to section 23 of the Act.

ACCESS RIGHTS AND CORRECTION

The BC Freedom of Information and Privacy Association (BCFIPA) and the BC Civil Liberties Association (BCCLA) proposed two amendments to ensure that people have effective rights of access to their personal information and the right to demand that it be corrected where it is false.

The first amendment relates to the access exception in section 23(4)(d) that stipulates that an organization must not disclose personal and other information to an individual "if the disclosure would reveal the identity of an individual who has provided personal information about another individual and the individual providing the personal information does not consent to disclosure of his or her identity."

The two privacy advocacy groups stated their position on this provision in the following way:

> *This exception is excessive and unfair. It would prevent individuals from obtaining access to vital information and opinions about themselves if it would reveal the identity of individuals who provided the information – even if the information were seriously in error or provided in bad faith. It could prevent the requesters from understanding and having the opportunity to correct information about themselves that may be used to make important decisions about them.*
>
> *We understand that access to one's own information should sometimes be limited in order to protect a third party who is a source of information. However, we think this should apply only where a clear case can be made that the third party or another specific interest will be harmed, and where the potential of harm is sufficiently serious to merit overriding an individual's normal right of access.*
>
> *Recommendation 3:*
> *Amend section 23(4)(d) of PIPA so that an individual may be denied access to their personal information only where a clear case can be made that the third party or another specific interest will be harmed, and where the potential of harm is sufficiently serious to merit overriding an individual's normal right of access.*[40]

The BCFIPA and BCCLA also proposed an amendment to s. 24(3), which stipulates that in the event that an organization makes no correction, "the organization must annotate the personal information under its control with the correction that was requested but not made". In their view, this subsection limits an individual's right to correction of personal information:

> *There has often been disagreement between complainants and organizations over the nature, prominence and placement of annotations that should be required under s. 24(3). We recommend that PIPA be amended so as to require that such notations be "easily apparent". This may not seem at first glance to be sufficiently important to warrant an amendment, but we can assure the members of the Special Committee that it*

[40] BCFIPA/BBCLA Joint Submission, pp. 9-10.

is extremely important to individuals about whom critical decisions may be made based on the contents of a file.

Recommendation 4:
That when a correction is requested under s. 24 of PIPA, the annotation of a correction that was requested but not made must be added to the personal information of the complainant in such a way and in such a location as to be easily apparent when the information is examined by any potential viewer.[41]

The Committee is not persuaded that the privacy advocacy groups have made a compelling argument for amending sections 23(4)(d) and 24(3). We think the wording of the existing provisions is adequate to protect access rights. Since we want to avoid making the provisions of the PIPA too prescriptive, we recommend that:

21. no amendments be made to sections 23(4)(d) and 24(3) of the Act.

"WITHOUT PREJUDICE" DISCUSSIONS

The Committee considered a proposal to add access exceptions for "without prejudice" discussions. Some members of the BC Branch of the Canadian Bar Association felt strongly that there should be an exception to the right of access for communications which are sent "without prejudice" (e.g., grievance settlement discussions, settlement privilege documents) as there is for solicitor-client privilege [s. 23(3)(a)]. They argued that this exception would promote the full and frank discussion of issues and encourage parties to resolve disputes at an early stage, without litigation.[42]

However, the Commissioner's Office rejected the idea that there should be an exception to an individual's right of access to her or his own personal information respecting communications that have been sent "without prejudice" in the context of settlement discussions in litigation or labour relations grievances. The Office does not see how this limitation on an individual's right of access is necessary to encourage early settlement of disputes, and is aware of no evidence that the right of access has been exercised in a way that prolongs disputes or prevents their resolution.[43]

The Committee agrees with the Commissioner's position and recommends that:

22. no amendment be made to the Act in relation to an access exception for "without prejudice" discussions.

[41] BCFIPA/BCCLA Joint Submission, p. 10.
[42] CBABC Submission, p. 2.
[43] OIPC Submission, p. 22.

ACCESS RIGHTS AND LITIGATION

During our discussion of witness statements, reference was made to the request of the Insurance Bureau of Canada for an access exception relating to litigation (see page 17). The Canadian Life and Health Insurance Association Inc. (CLHIA) had similar concerns about access rights and litigation and expressed the industry's position in the following way:

> *There is a growing base of experience within the industry where the access rights provided by the PIPA (and other private sector privacy legislation, for that matter) are being used for purposes that may have not been intended when the PIPA was enacted.*
>
> *One of the observable results is that the plaintiff bar is making more and more use of the new privacy legislation to obtain pre-litigation disclosure, at minimal cost, and thereby circumventing the discovery process that has long been in place to serve that very purpose. The life and health insurance industry has found that this is becoming more and more commonplace, particularly in relation to situations where there is a fair probability that the individual may ultimately begin litigation against the insurer. Insurers have received identical and detailed requests for access, clearly prepared by members of the plaintiff bar, which appear to be using the access request route as "fishing expeditions" to obtain information that would otherwise, and properly, be accessible through the discovery process, and then only if relevant.*
>
> *At the present time, Quebec's Act contains a provision that addresses this type of situation to some degree. Subsection 39(2) of that Act provides that a person carrying on an enterprise may refuse to communicate personal information to the person it concerns where disclosure of the information would be likely to "affect judicial proceedings in which either person has an interest". That provision requires that there be a serious indication that proceedings will initially be commenced based on the facts of the case.*
>
> *The industry suggests that consideration be given to adding a similar provision to section 23(3) of the PIPA to provide that an organization may refuse to provide access to personal information in the situations described above.*[44]

However, the Commissioner's Office believes no case of real need has been made for this significant change and opposes this recommendation, which has not been made in other privacy law review processes. For these reasons, the Committee recommends that:

23. no provision be added to the Act permitting the litigation process to supplant individuals' right of access to their own personal information.

ACCESS RIGHTS AND MEDICAL INFORMATION

The Committee considered another request from the CLHIA relating to access rights and medical information. Its submission pointed out that medical information held by a life and health insurer can be of a very sensitive nature and, in most circumstances, can be fully understood and explained only by a medical practitioner — for example, when the information tells the individual that they have "a dread disease" and have only months to live.

[44] CLHIA Submission, pp. 6-7.

The CLHIA acknowledged that the BC PIPA recognizes, to some degree, the importance of having a medical practitioner act as a conduit in providing access to medical information. The relevant provisions are section 23(4)(b), as well as section 5 of the Regulations, which allows for health care information to be disclosed to a health care professional prior to disclosing information under section 23. However, according to the CLHIA, this provision [s. 5(1), Regulations] sets a very high legal test (e.g., "grave and immediate harm") as well as complicated administrative thresholds (e.g., obtaining an assessment from the practitioner; entering into a confidentiality agreement) for allowing a company to disclose the information in a timely manner to an individual that has asked for access.

The insurers' position is that the approach described in Principle 9 of Schedule 1 of the PIPEDA would be more appropriate (ref. clause 4.9.1 provides, in part, that "the organization may choose to make sensitive personal information available through a medical practitioner".) "Consequently, the CLHIA recommends that PIPA's provisions in this regard be streamlined in order to ensure that the medical information can be properly explained to the individual and to allow the access request to be met in a timely manner."[45]

After carefully considering this request, the Committee is not persuaded that an amendment is necessary. Therefore we recommend that:

24. no amendment be made to section 23(4)(b) of PIPA or section 5(1), PIPA Regulations.

FEES FOR ACCESS

The question of fees for access to personal information was also considered. Under section 32(2) of the PIPA, an organization may charge an individual "a minimal fee" for access to personal information, but not for processing a request for employee personal information concerning the individual. The Act establishes certain rules respecting fees, such as requiring an organization to provide a written estimate before processing a request.

The Committee received a request for an amendment to the PIPA to give an employer the ability to impose a fee when a former employee makes an access request. Since the Act's rules do not apply in the case of former employees, we decided not to accept the proposal.

We did consider a request from the insurance industry to consider allowing an organization to charge "a reasonable fee" for access to records. The Insurance Bureau of Canada (IBC) pointed out that section 32(2) of the PIPA currently states that an organization may only charge an individual a "minimal fee" for providing access to that individual's personal information. In the IBC's view, a "minimal fee" is unreasonable in the context of a large or complex insurance claims file where the insurer must collect numerous different types of personal information in order to investigate and settle the claim. It prefers the approach taken in section 32(1) of the Alberta PIPA where an organization may charge a "reasonable fee". Therefore the IBC recommends that section 32(2) of

[45] CLHIA Submission, p. 9.

the BC PIPA be amended to provide that the organization may charge a reasonable fee for responding to access requests.[46]

This suggestion is supported by Commissioner's Office since it is concerned that the PIPA is "inconsistent" on the issue of fees (section 32(2) permits an organization to charge a minimal fee, yet section 36(2)(c) gives the Commissioner power to investigate whether a fee is "reasonable"). "Noting that Alberta PIPA permits the charging of a "reasonable" fee, the OIPC supports the IBC's suggestion that s. 32(2) be amended to provide clarity, by substituting "reasonable" for "minimal"."[47]

However, the Committee has reservations about supporting a fee hike that could potentially affect the ability of some individuals to access their own personal information. In our view, retaining a "minimal fee" acknowledges the entitlement that a person has to that information, and we also think the reasonableness test in section 36(2)(c) is appropriate. Therefore we recommend that:

25. no change be made to the "minimal fee" referred to in section 32(2) of the Act.

[46] IBC Submission, p. 6.
[47] OIPC Submission, p. 30.

OVERSIGHT PROVISIONS

Parts 10 and 11 of the Act provide for independent oversight by the Commissioner. In addition to general powers, the Commissioner has the power to authorize a private-sector organization to disregard requests and the powers to conduct investigations, audits and inquiries.

DISPUTE RESOLUTION PROCESS

The OIPC submission proposes "a complete re-build" of Part 10 – Role of Commissioner and Part 11 – Reviews and Orders to streamline the dispute resolution process for privacy complaints along the lines recommended by the 2004 FIPPA Review Committee. Making these parts congruent with the FIPPA would streamline the administration of the province's two privacy laws.[48]

For further clarification, the Committee asked the Commissioner what impact the FIPPA amendments contained in Bill 13, Labour and Citizens' Services Statutes Amendment Act, 2008 will have, if any, on his sweeping proposal to re-build Parts 10 and 11. His response indicated that Bill 13 contains some, not all, of the 2004 FIPPA Review Committee recommendations relating to the Office's powers and processes.

The Committee supports the Office's streamlining proposal because it would make the legislation more accessible and understandable to the general public. Based on our own experience of navigating the PIPA and FIPPA, we think having uniform provisions in both the private- and public-sector laws would be a positive step for the province to take. Therefore, to promote clarity and further harmonization, we recommend that:

26. government consider aligning the relevant provisions of the PIPA and the FIPPA in relation to the dispute resolution process for privacy complaints.

EARLY DISMISSAL OF COMPLAINTS

Section 37 of the Act currently allows an organization to ask the Commissioner for authorization to disregard an access request on the grounds that it is "frivolous or vexatious".

Like its Alberta counterpart, the Committee heard concerns that, in some cases, resources are being expended on investigations and inquiries that are unlikely to lead to effective resolution. The Canadian Bankers' Association, for example, proposed that the Commissioner be given the explicit authority to dismiss unsupported complaints in line with the approach recommended by the Alberta PIPA Review Committee.[49]

The Committee supports a similar amendment for the BC PIPA because we do not believe it is appropriate for the Commissioner's Office to spend time and money on unsupported complaints. Of course, this amendment does not preclude an individual bringing back a more substantial complaint for review. Therefore, in the interests of further harmonization with the Alberta PIPA, we recommend that:

[48] OIPC Submission, pp. 16-19.

[49] Recommendation 32, Alberta PIPA Review Committee Report, p. 35.

27. the Act be amended to provide the Commissioner with the explicit authority to discontinue an investigation or a review when the Commissioner believes the complaint or request for review is without merit or where there is not sufficient evidence to proceed.

SOLICITOR-CLIENT PRIVILEGE

The submission of the Law Society of British Columbia focused on the issue of solicitor-client privilege and, in particular, with the provisions set out in section 38 of the Act. It pointed out that section 38(3)(5) appears to authorize the Commissioner to require a law firm to produce client documents or information despite any privilege afforded by the law of evidence that may attach to such documents or information. On its face, therefore, this provision appears to be contrary to section 3(3) that provides that nothing in the Act affects solicitor-client privilege.[50]

However, the OIPC submission maintains that there is no inconsistency between the two sections and that solicitor-client privilege is well protected in the PIPA and so no amendment is necessary to fully protect the privilege.[51]

The Committee notes that on the topic of solicitor-client privilege, the Alberta PIPA Review Committee concluded that a legislative amendment should take into account any guidance offered by the Supreme Court of Canada in the case that concerns the power of the federal Privacy Commissioner to compel documents under the PIPEDA.[52] We have also learned that the Supreme Court of Canada ruling on this case is not expected to be made for several months.

On this issue, we support the position of the Commissioner's Office. We also believe solicitor-client privilege is the ultimate authority that any person enjoys and is fundamental to the relationship that every client has with her or his lawyer. Therefore, the idea that what a client discloses could be released in any way, shape or form without consent is difficult to contemplate. Accordingly, we recommend that:

28. no amendment be made to section 38(3)(5) of the Act.

INQUIRY PROCEDURE

The submission of a law firm noted that in recent decisions, the Commissioner has determined that under the legislation he has the ability not to proceed with an inquiry in certain circumstances. There have also been concerns raised about the time limits under which inquiries should be completed [see s. 50]. To remedy this, the law firm proposed the following amendments:

> *The legislation should be amended to make it clear that the commissioner's interpretation is the correct interpretation so that the commissioner's office is not subject to the potential of applications for judicial review to decide the commissioner's procedure.*

[50] Law Society of BC Submission, p. 2.
[51] OIPC Submission, pp. 13-14.
[52] Alberta PIPA Review Committee Report, pp. 35-36.

The commissioner should be given the ability under the legislation to reasonably determine his own process including the ability to determine and complete inquiries in a reasonable time frame without having a prescriptive or mandatory time imposed upon the office.

The Committee supports these sensible amendments and recommends that:

29. the Act be amended to clarify that the Commissioner has the discretion not to proceed with an inquiry in certain circumstances and the authority to reasonably determine his own process.

GENERAL PROVISIONS

Part 12 of the Act contains general provisions. The Committee considered requests relating to two section 56, Offences and penalties and section 58, Power to make regulations.

OFFENCES AND PENALTIES

A few witnesses suggested changes to the offence and penalty provisions in the Act. These included proposals to provide the enforcers of privacy and securities legislation with the ability to award substantial fines to organizations that fail to comply with valid direct requests of individuals seeking employee personal information.

After due deliberation, the Committee decided to recommend no legislative changes for the following reasons. First of all, we are not in favour of creating an enforcement arm in the Commissioner's Office that would require more resources to establish a process that could result ultimately in legal action. Secondly, and equally important, we think such an approach is contrary to the educational intent of the Act. In other words, rather than levying a fine to teach a self-regulatory organization a lesson, good practice results from assisting it to improve its policies and procedures. Therefore we recommend that:

30. no amendment be made to the Act in regard to offences and penalties.

PIPA REGULATIONS

The British Columbia Law Institute asked the Committee to consider a recommendation to broaden section 3 of the PIPA Regulations pertaining to who may act for a deceased person. Its submission pointed out that currently this section allows a personal representative or the nearest relative of a deceased person to exercise the rights the deceased person would have had to request personal information and consent to its release. However, it does not provide for cases of intestacy where there is no personal representative as yet, but someone is preparing to apply to court to be appointed the administrator of the estate. The applicant or his or her solicitor requires information about the deceased person's assets and liabilities in order to prepare the disclosure schedule required by the rules of court for an application for a grant of letters of administration.

The Law Institute then explained that in the course of its Succession Law Reform Project, it became clear from situations being encountered by the legal practitioners on its project committees that applications for letters of administration are being blocked because the exception in s. 3 of the PIPA Regulation is not broad enough. Financial institutions subject to PIPA and other entities holding financial information relating to the estate cannot see their way clear to release financial information about the deceased's estate to potential administrators of estates who do not fit into the definition of the "nearest relative" in the PIPA Regulations.

For legal practitioners, this creates a catch-22 situation, because an administrator of the estate of someone who dies intestate, in contrast to an executor appointed under a will, is not the personal representative until granted letters of administration by the court. A person cannot become the

administrator, however, without having access to financial information that is often being withheld because of PIPA requirements. In order to ensure that personal information relating to the estate need only be made to serious and legitimate applicants for administration and guard against frivolous or bad faith requests, the Law Institute recommendation is that s. 3 be widened to allow release of information when a request is made by a solicitor on behalf of a person intending to apply for a grant of administration.

The Committee supports this request because it will simplify procedure and make it easier for lawyers to draw up an appropriately accurate application for a grant of letters of administration. Accordingly, our final recommendation is that:

31. section 3 of the PIPA Regulations be amended to allow the release of information concerning the deceased's estate when a request is made by a solicitor on behalf of a person intending to apply for a grant of letters of administration.

SUMMARY OF RECOMMENDATIONS

The Special Committee to Review the Personal Information Protection Act recommends that:

Accountability for Cross-border Data Flows

1. section 4 of PIPA be amended to expressly provide that:

   (a) organizations are responsible for the personal information they transfer to a third party for processing or for providing services to or on behalf of the transferring organization; and

   (b) organizations must use contractual or other means to ensure compliance with PIPA, or to provide a comparable level of protection, for personal information they transfer to a third party for processing or for providing services to or on behalf of the transferring organization.

Mandatory Notification of Privacy Breaches

2. the PIPA be amended to include an express duty for organizations to notify affected individuals of unauthorized disclosure or use of their personal information. To be effective and not over-broad, the amendment should address the following considerations:

   (a) the kinds of personal information that must be involved before notice may be required, with personal information that is likely to create risks of financial loss or fraud and unauthorized disclosure of sensitive health information being key considerations;

   (b) who must be notified (affected individuals and the OIPC, with a possible added requirement to notify credit reporting agencies or law enforcement agencies in cases where financial loss is a risk);

   (c) how notice is to be given;

   (d) the timing of the giving of notice;

   (e) the general content of notices; and

   (f) authority for the Commissioner to order an organization to notify affected individuals of a privacy breach, on conditions the Commissioner may specify, where the organization has not given notice and the Commissioner considers that PIPA requires it.

Definitions

3. a definition of "destruction" not be added to the Act.

4. no amendment be made to the current definition of "investigation" in section 1.

5. the definition of "work product information" in section 1 be amended by adding "or compiled" to the clause "information prepared or collected".

Organization's Privacy Policies and Practices

6. no amendment be made to the Act requiring an organization to make written privacy policies publicly available.

Consent Provisions

7. section 11 be amended by adding "and necessary" at the end of the clause "a reasonable person would consider appropriate".
8. the Office of the Information and Privacy Commissioner consider developing an on-line resource guide, using the FAQ format, to educate private-sector organizations about the topic of information collection.
9. the Office of the Information and Privacy Commissioner consider using its website as the medium to encourage small business owners to use safer methods for processing credit and debit card transactions and to raise public awareness about the risks of discarding receipts.
10. the Act be amended to include a clause that prohibits blanket consent across financial pillars, and be reviewed for consistency with credit-reporting requirements in Part 6 of the *Business Practices and Consumer Protection Act*.

Exceptions to Consent

11. the Act be amended by adding a clause to sections 12, 15 and 18 to allow the collection, use and disclosure without consent of personal information necessary for the insurer to assess, adjust, settle or litigate a claim under an insurance policy.
12. no amendment be made to section 18(1)(j) of the Act.
13. "a reasonably contemplated" proceeding be added to the definition of "proceeding" in section 1 of the Act.
14. no amendments be made to the consent exceptions in sections 15(1)(c) and 18(1)(c) of the Act.
15. no amendments be made to the consent exceptions in sections 12(1)(e), 15(1)(e) and 18(1)(e) of the Act.
16. section 20 of the Act be amended to provide that an organization may disclose or collect, without consent, personal information in its custody or under its control (including personal information about its employees, customers, directors, officers or shareholders) that is reasonably required to be disclosed or collected in conjunction with a business transaction.
17. section 21(1)(b) of the PIPA be repealed and replaced with a provision stating that personal information can only be disclosed for research contact purposes with the approval of the Commissioner according to criteria set out in the Act or by regulation.
18. no amendment be made to section 22(c) or 22(d) of the Act at this time.
19. the PIPA be amended to permit non-consensual use and disclosure of "employee personal information" after termination of the employment relationship where the use or disclosure is necessary to manage post-employment relations or dealings between the employer and former employee.

Access-related Topics

20. no amendment be made to section 23 of the Act.

21. no amendments be made to sections 23(4)(d) and 24(3) of the Act.

22. no amendment be made to the Act in relation to an access exception for "without prejudice" discussions.

23. no provision be added to the Act permitting the litigation process to supplant individuals' right of access to their own personal information.

24. no amendment be made to section 23(4)(b) of PIPA or section 5(1), PIPA Regulations.

25. no change be made to the "minimal fee" referred to in section 32(2) of the Act.

Oversight Provisions

26. government consider aligning the relevant provisions of the PIPA and the FIPPA in relation to the dispute resolution process for privacy complaints.

27. the Act be amended to provide the Commissioner with the explicit authority to discontinue an investigation or a review when the Commissioner believes the complaint or request for review is without merit or where there is not sufficient evidence to proceed.

28. no amendment be made to section 38(3)(5) of the Act.

29. the Act be amended to clarify that the Commissioner has the discretion not to proceed with an inquiry in certain circumstances and the authority to reasonably determine his own process.

General Provisions

30. no amendment be made to the Act in regard to offences and penalties.

31. section 3 of the PIPA Regulations be amended to allow the release of information concerning the deceased's estate when a request is made by a solicitor on behalf of a person intending to apply for a grant of letters of administration.

APPENDIX A: SCHEDULE OF MEETINGS

May 3, 2007	Victoria	Organization
May 16, 2007	Victoria	Briefing
May 29, 2007	Victoria	Briefing
November 7, 2007	Victoria	Briefing
February 6, 2008	Victoria	Public Hearing
February 22, 2008	Vancouver	Public Hearing
March 13, 2008	Victoria	Deliberations
April 2, 2008	Victoria	Deliberations
April 8, 2008	Victoria	Deliberations
April 10, 2008	Victoria	Deliberations
April 15, 2008	Victoria	Deliberations Adoption of Report

APPENDIX B: WITNESS LIST

PUBLIC HEARINGS

Bart Armstrong, 06-Feb-08 (Victoria)

Association of Fundraising Professionals for Vancouver Island, Mandy Parker, 06-Feb-08 (Victoria)

British Columbia Cancer Agency/British Columbia Cancer Research Centre, Richard Gallagher, 22-Feb-08 (Vancouver)

British Columbia Freedom of Information and Privacy Association/British Columbia Civil Liberties Association, Darrell Evans, 22-Feb-08 (Vancouver)

Canadian Identity Resources Inc., George Greenwood, 22-Feb-08 (Vancouver)

William Gibbens, 22-Feb-08 (Vancouver)

Insurance Brokers Association of British Columbia, Laura Knight, 06-Feb-08 (Victoria)

Insurance Bureau of Canada, Serge Corbeil; Steven Lingard, 22-Feb-08 (Vancouver)

Anne Landry, 22-Feb-08 (Vancouver)

National Association for Information Destruction-Canada, Sheldon Greenspan, Robert Johnson, 06-Feb-08 (Victoria)

Roger Phillippe, 06-Feb-08 (Victoria)

United Auto Trades Association of British Columbia, George Hancock, Gerry Preddy, 06-Feb-08 (Victoria)

WRITTEN SUBMISSIONS

OIPC Submission

Office of the Information and Privacy Commissioner for British Columbia, David Loukidelis

Public Submissions

Joyce Anderson, Sub # 2

British Columbia Freedom of Information and Privacy Association/British Columbia Civil Liberties Association (Joint Submission), Darrell Evans, Sub # 30

British Columbia Law Institute, Greg Blue, Sub # 27

British Columbia Medical Association, Dr. Geoff Appleton, Sub # 19

David Buchanan, Sub # 18

Canadian Bankers Association, Linda Routledge, Sub # 15

Canadian Life and Health Insurance Association Inc., Jodi L. Skeates, Sub # 14

S. Clark, Sub # 20

Jack Dawson, Sub # 12

Fasken Martineau DuMoulin LLP, Lorene Novakowski, Sub # 13

William Gibbens, Sub # 28

David J. Huntley, Sub # 26

Insurance Bureau of Canada, Lindsay Olson, Sub # 10

Investorvoice.ca, Robert Kyle, Sub # 31

Don Johnson, Sub # 23

Grace Joubarne, Sub # 22

Gabriella Lang, Sub # 1

Mutual Fund Dealers Association of Canada, Shaun Devlin, Sub # 17

National Association for Information Destruction-Canada, Dave Carey, Sub # 24

Roger Phillippe, Sub # 5

Christine Seaville, Sub # 4

Sinnott & Company Law Corporation, Susan Sinnott, Sub # 9

Tony Staley, Sub # 21

The Canadian Bar Association, BC Branch, Freedom of Information and Privacy Law Section, Cappone D'Angelo, Janina Kon, Sub # 25

The Canadian Medical Protective Association, John E. Gray, Sub # 7

The Law Society of British Columbia, John Hunter, Sub # 11

Dr. Thomas Varzeliotis, Sub # 16

Barbara Westlake, Sub # 29

Robert Wong, Sub # 3

Wyder Management Ltd., Bruce Wyder, Sub # 6

Alex Yakunin, Sub # 8