THIRD LEGISLATIVE REVIEW OF THE

FREEDOM OF INFORMATION AND PROTECTION OF PRIVACY ACT

SUBMISSION OF THE

CANADIAN BAR ASSOCIATION, BC BRANCH

FREEDOM OF INFORMATION AND PRIVACY LAW SECTION

March 15, 2010

THE CANADIAN BAR ASSOCIATION
British Columbia Branch

March 15, 2010

Via Email

Special Committee to Review the Freedom of Information and Protection of Privacy Act
Office of the Clerk of Committees
Room 224, Parliament Buildings
Victoria, BC V8Y 3E1

Attention: Ron Cantelon, Chair

Re: Review of the *Freedom of Information and Protection of Privacy Act*

The Freedom of Information and Privacy Law Section of the Canadian Bar Association, British Columbia Branch ("CBABC") is pleased to respond to the call for submissions of the Special Committee to Review the *Freedom of Information and Protection of Privacy Act* ("**FIPPA**" or the "**Act**") on the occasion of the third legislative review of the Act.

The Canadian Bar Association represents 38,000 lawyers, judges, notaries, law teachers, and law students from across Canada, of which more than 6,400 are members of the BC Branch. The purposes of the Association include, among other things, enhancing the professional and commercial interests of our members, promoting fair justice systems and facilitating effective law reform.

The Freedom of Information and Privacy Section of the CBABC (the "Section") is comprised of members of the CBABC who share an interest or practice law in areas that pertain to freedom of information and privacy issues generally. Our membership, however, represents a vast range of perspectives on these issues, such that it would be a challenge for the Section to make specific recommendations to the Special Committee on any particular issue. Accordingly, rather than attempt to reconcile disparate points of view, the Section Executive sought to identify FIPPA issues that we felt may be of particular interest to the Special Committee, and to elicit feedback from our members on these issues. This submission is the product of both a broad Section meeting and multiple smaller working group sessions, and is intended to reflect the views of individual section members, rather than the views of the CBABC itself. We are grateful to all of our members who contributed to this process, and our hope and intention is that we have provided the Special Committee with a helpful perspective on the legislation and the areas that may require clarification or improvement.

Finally, this submission has been presented largely in summary form. We would, however, be pleased to address the Special Committee, either in person or in writing, in order to provide any clarification or additional information that may be of assistance to the Special Committee as it undertakes this legislative review.

Yours truly,

Alexis Kerr
Co-Chair, Freedom of Information and Privacy Law Section
Canadian Bar Association, BC Branch
Contact Information:
Fraser Health Authority
Tel.: 604-587-4671

And

Janina Kon
Co-Chair, Freedom of Information and Privacy Law Section
Canadian Bar Association, BC Branch
Contact Information:
Streamline Counsel Inc.
Tel.: 604-676-1450

CONTENTS

1. Mandatory Privacy Breach Notification

A number of the Section members had views about whether FIPPA should be amended to include a mandatory privacy breach notification obligation. FIPPA is currently silent on the issue of whether notification of a privacy breach to affected individuals should be made mandatory.

Currently Alberta and Ontario have legislation that requires mandatory notification of breaches. Recent amendments to Alberta's PIPA[1] requires notification "without unreasonable delay" to the Commissioner of any incident involving the loss of or unauthorized access to, or disclosure of, personal information where a reasonable person would consider that there exists a "real risk of significant harm" to an individual as a result of the loss or unauthorized access or disclosure. Ontario's Personal Health Information Protection Act provides that individuals must be notified of unauthorized disclosures "at the first reasonable opportunity".[2] Other jurisdictions, such as BC, have produced guidelines encouraging notification, which will enable individuals to limit the risk of harm that may ensue.

Those members supporting the imposition of mandatory privacy breach reporting noted the significant harm that can be caused to individuals from risks such as identity theft or other unauthorized uses of personal information.[3] These members also referred to recent media accounts of breaches and investigations by Privacy Commissioners highlighting the risks from unauthorized disclosures and lack of security precautions.[4]

Organizations can act to mitigate the risk of harm to individuals in the event of a privacy breach, by notifying the individuals affected. This way the individuals can take their own steps to reduce harm and to protect themselves. However, organizations may be reluctant to notify those affected, where it could negatively impact the organization, for example cause loss of trust or give rise to negative media attacks.

A number of members of the Section were also concerned, however, that any mandatory breach reporting that might be imposed not create a significantly different standard than that which exists in other jurisdictions. These members noted that the American experience with breach notification has been complicated by the varying reporting thresholds that have been implemented by different standards. There was concern expressed about the importance of consistency on this issue on a national scale.

The Office of the Privacy Commissioner of Canada is currently reviewing mandatory breach notification under PIPEDA, but this work is not yet concluded. The CBA National Privacy and Access Law Section (the "National Section") has been consulted by the Uniform Law Conference concerning the draft *Uniform Law Act*, which is aimed at harmonizing breach

---

[1] The *Personal Information Protection Amendment Act, 2009* which includes new mandatory breach notification provisions received Royal Assent on 26th November, 2009.

[2] Section 16(2) of *PHIPA.*

[3] http://www.ehealthinformation.ca/

[4] For example, OIPC Investigation Reports F10-01; F10-02.

notification across the private sector in Canada.[5] Under the draft legislation, notification is based on the risk of significant harm to the individuals to whom the information relates, notification to the Commissioner is required and there are proposed penalties for non-compliance. The Special Committee may wish to consider some of the operational issues and questions raised in the interim report produced by the working group appointed by the Uniform Law Conference and the advantages and disadvantages of the proposed approach.[6]

In June 2008, the National Section made submissions with respect to reform of the federal *Privacy Act* with respect to statutory breach notification. The CBA recommended an amendment to require federal institutions to notify individuals of unauthorized disclosures and that a balanced approach be adopted. That submission noted that important factors to take into account would be the number of individuals affected, the sensitivity of information and the probability of improper access. Other considerations would be the content of reports to the Commissioner and penalties for non-compliance.

Members of our Section also submitted comments to the Special Committee reviewing the *Personal Information Protection Act* ("PIPA") in February 12, 2008. At that time, as now, members had disparate views about mandatory breach notification, some preferring not to amend the legislation due to the difficulty in articulating a clear threshold requirement and of creating notification fatigue, or because they considered that the duty is already implied, and others supporting mandatory notification as a corollary of the principle of consent and right to know about a breach affecting them. Some considered the prospect of mandatory reporting becoming a standard approach and if so, supported harmonization with the Personal Information Protection and Electronic Documents Act ("PIPEDA") and provincial private sector privacy laws.

The issue of mandatory notification of privacy breaches was discussed at length by the former Information and Privacy Commissioner for BC in his submissions with respect to PIPA in 2008.[7] Section 34 of PIPA requires an organization to "protect personal information in its custody or under its control by making reasonable security arrangements to prevent the unauthorized access, collection, use, disclosure, copying, modification or disposal or similar risks". These provisions are substantially similar to those in section 30 of FIPPA, which requires a public body to "protect personal information in its custody or under its control by making reasonable security arrangements against such risks as unauthorized access, collection, use, disclosure or disposal".

In his submissions on PIPA, Commissioner Loukidelis (as he then was) was of the opinion that section 34 (corresponding to s. 30 in FIPPA), imposes a duty to notify in appropriate circumstances. Nevertheless, he submitted that there were reasons to clarify PIPA by including an express duty to notify *in carefully specified circumstances.* This would remove any uncertainty about the interpretation of that section to include such a duty and clarify the circumstances in which notification would be required. It would also be in line with recent changes to Alberta's PIPA and recommendations for reform of PIPEDA and be consistent with the move to harmonize private sector privacy laws.

---

[5] http://www.tclg.org/past-meetings/presentations/2009-mar-draftstatute.pdf

[6] Supra, note 5.

[7] Submission of the Office of the Information and Privacy Commissioner for British Columbia, March 2008, at page 12.

More specifically, the former Commissioner recommended that any amendment address:

- the kinds of personal information that must be involved before notice may be required, with personal information that is likely to create risk of financial loss or fraud being a key consideration
- who must be notified (individuals and the OIPC) and possible credit agencies and law enforcement)
- how notice would be given and timing of the notice
- the general content of notices
- authority for the Commissioner to direct an organization to comply

The Commissioner was concerned however about a broad requirement for the OIPC to decide in all cases that notification is *required* as this would not be an appropriate role for that office and would overburden it. The Special Committee appointed to review PIPA agreed generally with the Commissioner's recommendations.[8]

Some members of the Section agree with the practical approach of the Commissioner with respect to mandatory notification for both the public and private sector and recommend aligning both FIPPA and PIPA to create a consistent approach that is practical and workable for public bodies and private organizations alike. Those members view the trend towards mandatory breach reporting as something that will inevitably impact both the public and private sector and that the public interest would be well served by a mandatory provision that was framed in practical terms, but which did not mandate notification of *all* breaches. Some felt mandatory reporting to the Commissioner would enhance public body accountability; others felt that this was too onerous and inappropriate for his office.

Others expressed concern about the burden that would be placed on public bodies, particularly those will lesser resources, and the challenges of creating too many prescriptive rules around breach notification given the variable factors involved in a privacy breach. They cautioned the need for prescriptive rules given that there is already an inherent duty to notify embedded within section 30.

The Special Committee may wish to consider the different approaches to breach notification and reporting to the Commissioner in jurisdictions which have mandatory breach reporting to assess the practicality of these options.

---

[8] Streamlining British Columbia's Private Sector Privacy Law, Report of the Special Committee dated April 2008, at page7.

2. Extra-Territorial Data Transfers

In 2004, FIPPA was amended to address public concerns regarding the disclosure by the public sector of personal information to U.S.-based or other foreign-based service providers or their affiliates. The concern stemmed from a piece of legislation, known as the *USA PATRIOT Act*, which was enacted by the U.S. Houses of Congress following the events of September 11, 2001 to expand intelligence gathering and surveillance powers of law enforcement and national security agencies under the *Foreign Intelligence Surveillance Act* ("**FISA**"). The *USA PATRIOT Act* enlarged FISA's powers, for example, by lowering the threshold for judicial oversight over such activities and by broadening the methods and powers by which surveillance is conducted by authorities.

In 2004, the *USA PATRIOT Act* became the focal point of a highly publicized case in which it was argued that the outsourcing of public services by the Province through U.S.-linked service providers would expose personal information about British Columbians to disclosure under the *USA PATRIOT Act* in violation of FIPPA and the *Charter of Rights and Freedoms.*

Following a public consultation process, the Legislature enacted amendments to FIPPA to protect against the potential seizure of personal information pertaining to British Columbians by U.S. law enforcement officials. Among other things, these amendments imposed geographical restrictions on a public body for the custody of and access to personal information. The central amending provision appears at section 30.1 but also involves a number of ancillary provisions (collectively the "**Patriot Act Provisions**"). Section 30.1 of the Act reads as follows:

> **30.1** A public body must ensure that personal information in its custody or under its control is stored only in Canada and accessed only in Canada, unless one of the following applies:
>
> > (a) if the individual the information is about has identified the information and has consented, in the prescribed manner, to it being stored in or accessed from, as applicable, another jurisdiction;
> >
> > (b) if it is stored in or accessed from another jurisdiction for the purpose of disclosure allowed under this Act.
> >
> > (c) if it was disclosed under section 33.1(1)(i.1).

The Patriot Act Provisions affected many public bodies in BC who used information technology service providers with facilities outside Canada. These service providers from time to time required access to a public body's systems from outside Canada for maintenance or troubleshooting purposes. In response to concerns raised by public bodies that the Patriot Act Provisions were too restrictive, in 2006 the legislature passed amendments to FIPPA that permitted access and disclosure outside Canada under certain specific circumstances, including (1) to facilitate temporary travel outside of Canada by public body officials who require access to personal information while outside of Canada; (2) to facilitate temporary access by service providers when located outside of Canada; (3) to facilitate temporary access for the purposes of installing, maintaining or trouble-shooting electronic systems or for data recovery purposes.

The perspective of many of the Section's members was that, notwithstanding the 2006 amendments, public bodies and their service providers have struggled with compliance with the

USA Patriot Act Provisions, and compliance has often been achieved only by alteration of standard service provider arrangements, involving increased costs to the public body and significant risk to foreign-based or affiliated entities. The Patriot Act Provisions create a potential dilemma for foreign and U.S.-based or affiliated (and other foreign based or affiliated) entities of either breaching FIPPA or breaching the laws in their originating jurisdiction. Some service providers have, at considerable cost, responded by adopting elaborate corporate structures designed to insulate records from the reach of foreign law enforcement authorities. Many service agreements with such foreign affiliated entities also carry significant sanctions (including summary termination) for any failure to comply with the Patriot Act Provisions. These issues have the ability to impact the willingness of foreign entities to conduct business within British Columbia.

The Patriot Act Provisions prohibit access to and storage of personal information from outside of Canada, except in the narrow circumstances listed above. Many members felt that issues relating to access and storage of personal information outside Canada will only increase in coming years, With the rise in "cloud computing", data is becoming even more fluid across geographic boundaries. To cite an example, the BC Government recently issued a ministerial order in response to concerns that the Patriot Act Provisions prevented public bodies from using social media sites such as Facebook, Twitter and MySpace to engage members of the public. The ministerial order, issued on December 17, 2009 under s. 33.1(3) of FIPPA, permits public bodies to disclose personal information outside of Canada through social media sites as long as the disclosure meets prescribed conditions. A copy of the Ministerial Order can be found on the internet at http://www.cio.gov.bc.ca/services/priva ... 091217.pdf

Since 2004 there have been some modifications to the USA PATRIOT Act which have affected some of the original areas of concern, although there is legitimate debate over whether there has been any meaningful change in the scope of potential risk under that legislation.

British Columbia was a pioneer in introducing specific legislation dealing with geographical restrictions on custody and access. Since then Nova Scotia has followed with a more modified and flexible version of BC's Patriot Act amendments. Section 5 of Nova Scotia's *Personal Information International Disclosure Protection Act*, S.N.S. 2006, c. 3 prohibits storage or access outside Canada, but allows the head of a public body to permit such storage or access "to meet the necessary requirements of the public body's operation." No other Canadian jurisdiction has introduced geographical restrictions on storage and access, although the provinces of Alberta and Quebec have introduced other types of provisions in response to the USA PATRIOT Act. For example, Alberta's *Freedom of Information and Protection of Privacy Act*, R.S.A. 2000, c. F-25 and its *Health Information Act*, R.S.A. 2000, c. H-5 create an offence for disclosing personal information pursuant to an order made by a body with no jurisdiction in Alberta. Other Canadian jurisdictions have generated policies and guidelines which take a more subjective approach to the issues of storage and access; as a result BC's rules in this area are the most prescriptive and restrictive in Canada.

Some members of the Section felt that the Committee should consider whether it wishes to revisit the policy issues surrounding the Patriot Act Provisions and whether BC's legislative approach is an appropriate tool for protecting the privacy and security of personal information.

Other members expressed concerns about the ability of public bodies to monitor compliance with arrangements for storage and access rights to data disclosed outside of Canada due to lack of resources and felt that there could be public discomfort with respect to data stored outside Canada, especially for research and other secondary uses.

The CBA is not able to take any position on that policy debate, as our organization includes members who are both supportive of and critical of the Patriot Act Provisions.

3. **Technology and FIPPA**

In recent years, the use and presence of technology within the public sector has proliferated with the uptake of remote access technology, increased use of the Internet and the exponential growth of electronic databases and interconnected systems, all of which continue to transform how public services are delivered. Access to a vast scope of information from inside and outside of the office has enabled changes to working practice and work flow. The scope of information now available electronically has accelerated integration of services and new research demands. Keeping pace with evolving database and system security requirements is a challenge for most public bodies.

As discussed in more detail below, a number of Section members felt that the language and concepts set out in FIPPA had not kept pace with these changing technologies. While the issue of changing technologies was the subject of comment in the report of the Special Committee to Review the Freedom of Information and Protection of Privacy Act in May 2004 (the "**2004 Report**"), a number of our members were of the view that further consideration should be given during this 2010 legislative review to amending the Act to address the impact of changing technologies on information management within the public sector.

(a) New Trends

Members of our Section observed some of the following trends relating to new information technologies:

- Electronic systems now co-exist with manual systems, creating the potential for different and inconsistent standards for data recording, processing and retention and for data integrity.

- Technology is expanding the scope and volume of information collection, use and disclosure among users in the public sector.

- With larger volumes of information being collected, it is becoming increasingly difficult to facilitate access requests. Conducting adequate searches for documents and emails is onerous and time-consuming for access to information staff, particularly with respect to complex requests.

- Advances in technology enable a vast scope of personal information about individuals to be stored and made accessible "from cradle to grave". Record retention is a growing issue in the public sector.

- The use of digital recording technologies and mobile technology is increasing in public bodies. The records created and/or stored using these technologies may be used for medical care, speech therapy and other assessments and for secondary uses.

- The use of shared or integrated databases for the management of records and personal information has increased, giving rise to lack of clarity around disclosure and access and custody and control as those concepts are raised under FIPPA.

Specific comments by members regarding potential amendments to FIPPA that might flow from this changing landscape are set out below.

(b) Disclosure and Access to Electronic Databases

A number of our members observed that the legislation might be improved by clarifying and/or adding to the concepts of disclosure and access in the context of shared electronic databases. Currently "access" is defined in the Act, but "disclosure" is not. In addition, the definition of access is somewhat circular. "Access" is defined as "disclosure of personal information by the provision of access to personal information".

One of our members noted that public bodies are becoming involved in setting up common databases as a means of facilitating the sharing of information that is required to provide integrated services to individuals. In the course of evaluating these systems, questions frequently arise as to whether, simply by inputting information into a database that is used by two or more public bodies or by enabling access to it by other public bodies, a public body is "disclosing personal information" within the meaning of the Act. There was some concern expressed that, in the use of shared electronic databases among two or more public bodies, there is a lack of clarity as to whether the potential for a user from another public body to "access" the information amounts to a "disclosure" and as to whether enabling access to a system by another public body, could be interpreted as the "provision of access" to that public body and its users and therefore a disclosure within the meaning of FIPPA.

The member suggested that merely inputting personal information into a database should not be construed as unauthorized disclosure as long as policies, agreements and technical controls are put into place which govern users' access to the information and limit it to situations where the access is authorized under FIPPA. Moreover, the mere creation of the database itself should not be considered a "disclosure" of the inputted data. It was suggested that the creation of the database should be regarded as simply an infrastructure for the potential sharing of personal information to the participating public bodies' users and it is only when a user accesses the information that a disclosure takes place. The issue of whether any particular access is authorized under FIPPA must be resolved through a legal analysis on a case-by-case basis.

Another member countered that providing such accessibility should not be permitted unless disclosure to the system users is authorized under FIPPA, for example, as part of an authorized, integrated program under section 33.2(d) of FIPPA. Inputting data into a database that is shared among public bodies means that information is released for access by these public bodies and may be subject to further disclosures. Public bodies should not be releasing data to others without doing their due diligence before they input the data.

A third member pointed out that, in practical terms, it may be difficult if not impossible for public bodies to ensure that they make accessible to each individual user only that personal information contained in a database that the user is authorized to access under FIPPA. Such authorization is often circumstance-based (i.e., it is limited by the "need-to-know" principle). Thus there might be a certain category of records that an individual user may legitimately need to access in order to perform his or her job function(s), however it will often be the case that the individual user does not have a need to access every record in that category.

It is suggested that the Special Committee may wish to consider amending the definition of "access" or introduce new language that deals with the issue of accessibility versus disclosure in the context of shared electronic databases.

(c) Information in "Manipulable" Form

Another technology related concern expressed by Section members relates to Part II of FIPPA (the access to information provisions), and members of the public who ask for disclosure of records in a specified electronic form.

Several members observed that members of the public seeking access to records under FIPPA have requested records in a particular electronic format, (such as Microsoft Access or Excel). Some public bodies have reservations about providing certain records in manipulable format, on the grounds that such records could be altered and used for fraudulent or other improper purposes. At least one member of the Section knew of a situation in which such misuse had occurred. In response to this concern, some public bodies release records electronically but in non-manipulable format (such as scanned PDF format).

A public body's obligation to create records in order to respond to an access request is addressed in section 6 of FIPPA:

> **6** (1) The head of a public body must make every reasonable effort to assist applicants and to respond without delay to each applicant openly, accurately and completely.
>
> (2) Moreover, the head of a public body must create a record for an applicant if
>
> (a) the record can be created from a machine readable record in the custody or under the control of the public body using its normal computer hardware and software and technical expertise, and
>
> (b) creating the record would not unreasonably interfere with the operations of the public body.

We note that one recent mediation conducted by the Office of the Information and Privacy Commissioner ("OIPC") addressed the issue of the obligation to create records in electronic format.[9] There, a news reporter requested information in Excel format so that he could construct a searchable database. Three of the public bodies responded with paper records, contrary to his request. The OIPC pointed out that section 6(1) of FIPPA requires a public body to make every reasonable effort to assist applicants and to respond without delay to each applicant openly, accurately and completely. Section 6(2) requires a public body to create a record for an applicant if doing so would not unreasonably interfere with the operations of the public body. In this case very little effort would be required to provide the records in Excel format. The matter was resolved with all three public bodies agreeing to release the records in electronic format. What is noteworthy about this Mediation Summary is that it implies that public bodies have an obligation under FIPPA to produce electronic records in the format requested by the applicant, so long as doing so would not unreasonably interfere with the operations of the public body.[10]

Some Section members suggested that FIPPA be amended to specify that public bodies may exercise their discretion, subject to such reasonable limitations as the Special Committee may see fit to impose, as to whether or not a record should be provided in manipulable format. This would allow public bodies to take reasonable steps to protect against misuse or alteration of the information in the records. Certain members felt that this discretion is of particular importance in situations where the applicant intends to enter the information in a database which will be widely available to the public through an open web site. One member suggested that FIPPA should include an offence, subject to monetary penalty, for intentional or fraudulent misuse by an applicant of records disclosed under the Act.

Other members suggested that meaningful access sometimes entails the ability to search and organize, in some cases electronically, the information provided by a public body. Public bodies should release information in a format that facilitates meaningful access to records, and should not stymie access by putting records into non-manipulable format. However, in some cases an applicant would have no legitimate reason to request a record in manipulable format. For example, a public body would be well-justified in releasing documents such as letters in paper or scanned PDF format.

(d) Purposes

Some members felt that the trends in new technology should be reflected in amendments to the purposes section of the Act. It was suggested that section 2 of the Act specifically acknowledge the importance of enabling technology to enhance access to information and privacy protections. Expressing this as a clear goal would support the use of technology to enhance access to

[9] Summary 14, OIPC 2008-2009 Annual Report p. 34.

[10] Two OIPC decisions are relevant to this issue. In Order 03-16, an applicant specifically requested records in electronic and not paper format. The Commissioner held that the public body was required under s. 6(2) to create the electronic record. However, the record could not reasonably be severed and so the public body was not required to respond to the request. In Order 03-19 the Commissioner held that the public body was required to create the electronic records requested, and that the 48 hours of programmer time required to fulfill the request would not unreasonably interfere with its operations. Neither decision touched on whether an applicant has the right to receive a record in a particular electronic format.

information and to protect personal information. Some members felt that further amendments might also speak in more detail to the reasonable security arrangements that are required to protect personal information in the custody or control of a public body and to address record retention for electronic records.

(e) Access Design Principles

It was also suggested by some members that to support transparency, an amendment to FIPPA should be considered to require that public bodies implement prescribed access design principles for information systems and programs, in order to facilitate access to information requests. This suggestion reflects recommendations made by the Commissioner during the 2004 legislative review. As the Commissioner observed in Order F03-1611:

> It is not an option for public bodies to decline to grapple with ensuring that information rights in the Act are as meaningful in relation to large-scale electronic information systems as they are in relation to paper-based record-keeping systems. Access requests like this one test the limits of the usefulness of the Act. This is as it should be. Public bodies must ensure that their electronic information systems are designed and operated in a way that enables them to provide access to information under the Act. The public has a right to expect that new information technology will enhance, not undermine, information rights under the Act and that public bodies are actively and effectively striving to meet this objective.

The suggestion was that information should be organized in a manner that allows for public dissemination and for public bodies to locate and readily access information in respect of which access requests may be made. The sophistication of these schemes will depend on the complexity of the information and the size and complexity of the public body. One member felt that, without guidelines, public bodies may build new systems without clear or consistent standards with respect to access to information. Members also pointed out that publication schemes have become established in other jurisdictions and that this would enhance the transparency and accountability of public bodies.[12]

Conversely, another member cautioned that the Special Committee should be wary of the resource implications that may follow from the imposition of such principles by way of legislation, particularly if such principles were to be made applicable retroactively to existing legacy systems. This member pointed out that in addition to accounting for the complexity of information and the size and complexity of the public body, the pace of change in technology itself must be considered as a factor in terms of whether legislation is the appropriate vehicle for communicating expectations in this regard.

[11] At para. 64.

[12] http://www.itspublicknoweldge.info/home/SICPublicationScheme/PSintro.asp

4. Integration of Service Delivery

Some Section members observed that there is an increasing trend within the public sector of the integration of services and programs between ministries and public bodies. This trend challenges the language in the Act which does not specifically anticipate the scenario in which possession, custody or control may be shared between public bodies. Under the current legislation, these integrated programs can leave unclear who has custody or control of records, and the extent to which responsibilities under FIPPA may be shared.

(a) Shared Control

Section 3 of the Act provides that the Act applies to all records in the "custody or under the control" of a public body. The terms 'custody' and 'control' are not defined by the Act and one must therefore look to case law and orders of the OIPC to better understand these concepts.[13]

A public body's obtains "custody or control" of records containing personal information through collection of the information consistent with its mandate and operating programs and activities.[14] However, some records or electronic systems may fall under the stewardship of one or more public bodies that share information for integrated programs and services. This raises questions about custody and control of records and how the integrated working teams respond to the exercise by individuals of their privacy and access rights under FIPPA.

Prior orders and reports of the OIPC have indicated that custody or control need not be exclusive.[15] Some members felt that this concept should be made explicit in FIPPA by including a provision which permits two or more public bodies to have shared custody or control of a record, including for the purposes of a common or integrated program or services under Part 3 of the Act. Some members also felt that the Act could elaborate about how to allocate responsibilities for compliance with FIPPA when a situation of shared custody and control arises.[16]

Some of our members also indicated that, where the issue of shared control arises between a public sector entity governed by FIPPA and a private sector entity governed by PIPA, it can also be challenging for the organizations to determine their respective rights and responsibilities under these statutes. The proliferation of various models of public-private partnerships within the public sector has led to an increasing number of such scenarios arising. Although many public bodies address this issue through contractual language with their private sector partners, some members felt that the Special Committee should also consider whether the issue of shared

---

[13] For example, B.C. Orders F02-29; F02-30; F06-01; and more recently **F10-01**. See also the preliminary decision by the Commissioner dated November 19, 2002 involving the College of Pharmacists and Ministry of Health Services in respect of the PharmaNet database.

[14] Section 26(c) of FIPPA.

[15] Order 04-19

control should be addressed to clarify the parties' rights and responsibilities in these circumstances. This might be considered in conjunction with the concept of "service provider" to a public body.

(b) Public Body as Service Provider

In light of the trend toward increasing integration of services or functions, some of the Section members also raised concerns about circumstances in which one public body becomes a "service provider" to another. These circumstances are arising with increasing frequency, and give rise to questions about whether the "service provider" by assuming physical possession of records from another public body in the course of performing services, also obtains "custody" for the purposes of section 3 of the Act.

Some Section members felt that it would assist to include a clarification in the Act that the public body functioning as "service provider" does not have "custody and control" of the records obtained in the course of service delivery. While there is case law that is supportive of that analysis, some of the Section members felt that legislative recognition of that interpretation would assist.

Indeed, we note that in the 2004 Report, the Special Committee recommended the inclusion of an amendment to section 3 of the Act specifically providing that personal information, created by or in the custody of a "service provider", would be considered under the control of the public body for whom the contractor is providing services.

However, others were concerned that permitting a public body to provide services on behalf of another public body could be inconsistent with the mandate of the public body appointed to provide the services and to the extent there is inconsistency between the service provider provisions and the authority for collection for operating programs and activities, this should be clarified.

(c) Common and Integrated Programs (s. 33.2(d))

While FIPPA does authorize the flow of information for integrated programs and service delivery, some members of the Section asserted that the language in the Act is vague and clarification may assist the parties in better understanding the scope and application of this authority for disclosure. Section 33.2(d) of the Act states as follows:

> A public body may disclose personal information referred to in section 33 inside Canada as follows:
>
> . . . (d) to an officer or employee of a public body or to a minister, if the information is necessary for the delivery of a common or integrated program or activity and for the performance of the duties of the officer, employee or minister to whom the information is disclosed;

The phrase "common or integrated program or activity" is not specifically defined in FIPPA, nor has it been clearly addressed in case law. Some members suggested that the addition of a definition of "common or integrated programs" may add clarity to the application of this section.

(d) Whistleblower Provisions

Section 30.3 of FIPPA prohibits an employer from disadvantaging or denying an employee a benefit because the employee, acting in good faith and on the basis of reasonable belief, has reported a contravention to the Commissioner or refused to do anything in contravention of FIPPA.

There was some support for the view that the whistle-blower protections should be clarified to cover any person who imposes retribution or other negative consequences rather than specifically limited these protections to the employer and employee relationship. As public bodies move towards increasing service integration, some Section members felt that appropriate protections are necessary to ensure that employers participating in integrated teams are subject to the same prohibitions with respect to any person who may be subject to their control or influence.

One member suggested that appointing Chief Privacy Officers to public bodies should be considered to oversee appropriate compliance with the Act. Another member felt that any amendment to FIPPA in this respect would be unnecessary, given that the Act currently assigns responsibility for compliance with the head of each public body.

5. Who Can Act for Young People and Others

In its May 2004 Report of the Special Committee to Review the *Freedom of Information and Protection of Privacy Act*, the Special Committee recommended that section 3 of the Freedom of Information and Protection of Privacy Act Regulation be amended to make it consistent with sections 1 to 4 of the Personal Information Protection Act Regulations. In making this recommendation, the Special Committee effectively endorsed the submission of the Information and Privacy Commissioner, whose concerns were that the existing provision did not recognize certain types of legitimate representatives (e.g a power of attorney or a representative under the *Representation Agreement Act*) nor did it rank "nearest relatives" in order of priority.

To date, this recommendation has not been acted upon.

There is support amongst the members of our Section for the Special Committee to reissue this recommendation. In particular, some of or members who have experience in applying section 3 of the FOIPP Regulation in the context of processing a freedom of information request agree that amending this provision to, in particular, clarify the priority of "nearest relatives" would assist public bodies to expedite the processing of certain requests. For example, upon the death of an individual, it is not uncommon for public bodies that have custody and control of records that may be relevant to the administration of the deceased person's estate (e.g. health authorities, social service providers, the deceased individual's employer) to receive one or more freedom of information requests for the deceased individual's records. Under the current provision, it is difficult for a public body to make a determination that the requester is actually making the request as the "representative" of the deceased individual, as opposed to making the request to serve a personal interest.

6. Privacy Impact Assessments

The Act currently includes a requirement that all Provincial ministries conduct privacy impact assessments ("PIA") in accordance with the directions of the responsible Ministry. It does not impose a corresponding obligation on other public bodies. There were disparate views among the members of the Section on whether conducting a PIA should be a mandatory requirement for all public bodies.

Some members felt that mandatory PIA's could be an important step in establishing consistently high privacy protections standards throughout the public sector in British Columbia. However, others indicated that this step is unnecessary, and would place too onerous an administrative burden on public bodies, particularly those public bodies that are either very small, or that handle little to no personal information. A number of our members also pointed out, that in their experience, PIAs are being conducted by many public bodies even without the existence of a statutory requirement.

A number of members also pointed out that, if a requirement is to be incorporated into the Act, it should be done in such a way to allow public bodies sufficient flexibility in conducting these processes. Those members were of the view that public bodies, themselves, should be left to determine how rigorous an assessment is appropriate to the given situation.

7. Minimum Standards for Information Sharing Agreements

Although the Act contains no blanket requirement that public bodies enter into information sharing agreements, there have been several OIPC decisions that have established that a public body which routinely provides personal information to service providers or other third parties should as part of its obligations under section 30 of the Act (reasonable security measures) enter into an information sharing agreement.

Some of our members were of the view that the Act could usefully include provisions establishing minimum standards for the content of such agreements. Some noted that section 19 of the *E-Health (Personal Health Information Access and Personal Privacy) Act*, which does mandate the use of information sharing agreements, includes a mandatory provision that might be used as a model for such language.

8. Labour Relations Information

Concern was also expressed about the treatment of labour relations disputes under the access to information provisions in Part 2 of the Act. While labour relations disputes are legal proceedings, they are typically not entitled to protection under section 14 (legal privilege) of the Act because employers are more often represented by managers or labour relations consultants rather than lawyers. While some protection to the disclosure of this information is offered under section 13 (policy advice and recommendations), it does not protect background facts from disclosure. As a result, such members noted that an unlevel playing field is created for

employers where unions can gain access, at least in part, to the employer's case through freedom of information requests.

In terms of suggesting an alternative approach, one member pointed out that the Ontario *Freedom of Information and Protection of Privacy Act*, R.S.O. 1990, c. F. 31 provides an exclusion (not exception) of labour relation records in the following manner:

> Subject to subsection (7), this Act does not apply to records collected, prepared, maintained or used by or on behalf of an institution in relation to any of the following:
>
> 1. Proceedings or anticipated proceedings before a court, tribunal or other entity relating to labour relations or to the employment of a person by the institution.
>
> 2. Negotiations or anticipated negotiations relating to labour relations or to the employment of a person by the institution between the institution and a person, bargaining agent or party to a proceeding or an anticipated proceeding.
>
> 3. Meetings, consultations, discussions or communications about labour relations or employment-related matters in which the institution has an interest. 1995, c. 1, s. 82.

9. Limiting Uses in Accordance with the Reasonable Expectations of the Public

Some of our members were also concerned about bringing greater clarity to determining permissible uses of information. In particular, it was noted in our discussions that the concepts of purposes for collection and consistent purposes are vague and can be challenging, and these concepts are important for establishing the limits on the use and disclosure of information in accordance with sections 32(a) and 33.2(a) of the Act. Some members noted that one of the tests that has been applied for determining whether a use of information is consistent with the purposes for collection is whether the use would meet a reasonableness threshold. These members also noted that imposing "a reasonable expectations" limitation on the use of information would not only add clarity to these concepts in FIPPA, but would also be consistent with similar language in section 14 of the *Personal Information Protection Act.* It states:

> Subject to this Act, an organization may use personal information only for purposes that a reasonable person would consider appropriate in the circumstances and that
>
> (a) fulfill the purposes that the organization discloses under section 10 (1),
>
> (b) for information collected before this Act comes into force, fulfill the purposes for which it was collected, or
>
> (c) are otherwise permitted under this Act.

We note, however, that our members had differing views about this issue. A number acknowledged the value of achieving consistence between the *Personal Information Protection Act* and FIPPA, but many felt that imposing a reasonableness requirement in addition to the other requirements of the Act would impose too great a burden on public bodies and would create greater uncertainty about the application of the Act. Others felt that the word "necessary" should

be defined to clarify the threshold to be applied to collection, use and disclosure of personal information.

10. Harmonization of PIPA and FIPPA

A number of our members expressed concerns about the importance of harmonizing the provisions of PIPA and FIPPA to ensure that, wherever possible or justifiable, applicant standards and thresholds are consistent. For example, our members observed the following potential inconsistencies between these statutes that the Special Committee may wish to consider:

- FIPPA requires that consent to uses and disclosure of personal information to be provided only in express written form, whereas PIPA allows consent to be provided in verbal form or to be implied.

- PIPA permits an employer to collect, use and disclose (without consent) personal information for the purposes of conducting an "investigation or proceeding". This language is broad enough to encompass employment related investigations for transgressions falling short of criminal activity or illegality. FIPPA permits a public body to collect, use and disclose personal information without the consent for the purposes of a law enforcement investigation. It is unclear or doubtful that this language would encompass employment investigations. On the other hand, some felt that it should be clear that employment investigations would not permit targeted or indiscriminate collection of information or monitoring that has no reasonable basis, particularly where employees have not been notified of such practices.

- As discussed in detail above, PIPA includes a general reasonableness threshold. FIPPA does not.

11. Health Care Specific Issues

A number of members from the Section had concerns about the need for special allowances to be made to address the particular issues that arise in relation to information sharing within the health care sector.

(a) Specific Health Privacy Legislation

In particular, many of our members were of the view that the Special Committee should carefully consider the experiences in those Canadian jurisdictions that have moved to enact specific health sector privacy legislation, such as Alberta, Saskatchewan, Manitoba, Ontario, Nova Scotia and Newfoundland.

Some of the concerns these members expressed included the fact that health care providers within the public and private sectors may require sudden and immediate access to health care records or information held by other health care providers. FIPPA (and/or PIPA) does not provide an efficient or seamless process by which this can occur.

While the recently enacted *E-Health (Personal Information Protection) Act* addresses some of the issues relating to the sharing of health information, its utility is limited to information that is retained within specifically designated health information banks. Some of our members felt that this legislation does not address the full range of information sharing needs within the health care sector and that the legislation should be extended beyond designated health information banks.

Others felt that Ontario and Alberta in particular have each elected to enact health care specific privacy legislation which creates more fluid processes for addressing health care related information exchanges. The Special Committee may wish to consider these different approaches and the experiences in other jurisdictions.

(b) Health Research and Health Planning

Some members expressed the view that there is a need for clarification in section 35 of the Act (Research) authorizing health care bodies and the Province to use health-related research for health planning purposes. Others felt that the *E-Health (Personal Information Protection) Act* addressed already presented an appropriate solution for these activities.

12. Section 16 - Disclosure Harmful to Intergovernmental Negotiations

Section 16 of the Act entitles public bodies to withhold information responsive to an access request if its disclosure would be harmful to relations between the government and the following agencies or reveal information provided by any of the following agencies.

(i) the government of Canada or a province of Canada;
(ii) the council of a municipality or the board of a regional district;
(iii) an aboriginal government;
(iv) the government of a foreign state;
(v) an international organization of states,

Some of our members felt strongly that this list of agencies was due for review, and that the role and scope of the entities now falling within the scope of FIPPA has changed since this provision was first drafted. These members felt that the Special Committee may wish to review whether this list should be updated to include other government agencies.

13. Section 21 - Third Party Business Information

Some Section members expressed concern over the high threshold established by case law for allowing information to be withheld under s. 21 of the Act. In particular, findings under the Act have made it very difficult for organizations to establish that information was “supplied in confidence”, as required by s. 21(1)(b), and to meet the harms test set out in s. 21(1)(c) of the Act. These Section members have asked that the Special Committee consider whether a legislative amendment would be appropriate to better protect the information of third party businesses.

One member also felt that section 21 should be redrafted in plain English so that it is more accessible to the reader. In particular, this member noted that certain OIPC interpretations of the phrase "*supplied in confidence*" is so narrow as to render meaningless its ordinary understanding in the business community. This member felt that it, if the intent is that virtually all third party business information provided to government is intended to be subject to public access, then, as a matter of fairness to the business community, words of section 21 should clearly express that intention.

However, other members noted that the 2004 Special Committee considered a similar submission and declined to recommend an amendment to s. 21. Some members expressed the view that FIPPA is meant to promote the transparency of public bodies, and that amendments to FIPPA should not detract from this transparency, and therefore amendments to s. 21 are not appropriate.

SUMMARY

All of which is respectfully submitted.