# SUBMISSIONS OF THE CANADIAN BAR ASSOCIATION (BRITISH COLUMBIA BRANCH)

TO THE SPECIAL COMMITTEE

TO REVIEW

THE FREEDOM OF INFORMATION AND PROTECTION OF PRIVACY ACT

Issued By:

Canadian Bar Association
British Columbia Branch

Special Committee of the
Freedom of Information and
Privacy Law Section

January 2016

# Table of Contents

## PREFACE

Formed in 1896, the purpose of the Canadian Bar Association (British Columbia Branch) (the "CBABC") is to:

- Enhance the professional and commercial interests of our members;
- Provide personal and professional development and support for our members;
- Protect the independence of the judiciary and the Bar;
- Promote access to justice;
- Promote fair justice systems and practical and effective law reform; and
- Promote equality in the legal profession and eliminate discrimination.

The CBA nationally represents approximately 39,000 members and the British Columbia Branch itself has over 6,900 members. Our members practice law in many different areas. The CBABC has established 77 different sections to provide a focus for lawyers who practice in similar areas to participate in continuing legal education, research and law reform. The CBABC has also established standing committees and special committees from time to time.

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 attempting to reconcile disparate points of view, the Section Executive decided to solicit and record input from individual members in its submissions to the Special Committee. As a result, the Section's submissions do not necessarily adopt a unified position on a particular issue. The following submissions reflect the views of individual Section members, and not necessarily the views of the CBABC or the Section as a whole.

The overall purpose of these submissions are not meant to be sweeping, but to: (1) clarify variations in application of the law gleaned from case law and orders, and (2) make the legislation more robust and current to keep pace with ever-changing technological advances.

We are grateful to all of our Section members who contributed to this process. We are especially thankful for the work of Selina Koonar. She co-chaired our Section working group and she has been instrumental in getting these submissions to completion. Our hope and intention is that in our submissions we have provided the Special Committee with a helpful perspective on the legislation and the areas that may require clarification or improvement.

## EXECUTIVE SUMMARY

Section members submitted comments in relation to six issues. First is the issue of the expansion of the access, storage and disclosure of personal information from outside Canada. Second is the application of FIPPA to wholly-owned subsidiaries of public bodies. The third issue is requirement to provide notice for collection of personal information in the context of confidential employment investigations. The fourth issue is the legislative language permitting access to documents otherwise protected by solicitor-client privilege. Fifth is the issue of mandatory breach notification. Sixth is the issue of the duty to document.

Some members proposed specific recommendations or drafted proposed amendments. These Proposals have been included, and are summarized at the end of this document, with a view to assisting the Special Committee in its work.

## SUBMISSIONS

The Section 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 fourth legislative review of the Act.

## A. EXPANSION OF ACCESS, STORAGE AND DISCLOSURE OF PERSONAL INFORMATION FROM OUTSIDE CANADA

Section 30.1 of FIPPA creates a near-absolute prohibition on the storage or access to personal information outside Canada. It reads:

> **Storage and access must be in Canada**
>
> 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).

Section 30.1 does not allow public bodies to store personal information outside Canada, or allow access to that information from outside Canada, except where the public body has secured written consent or in other limited circumstances listed under section 33.1, such as installing or fixing electronic systems (s.33.1(1)(p)), or processing credit card payments (s.33.1(1)(i.1)).

**Proposal 1**

For the reasons discussed below, some Section members recommended that FIPPA be amended to give public bodies discretion to store or access personal information outside Canada under limited circumstances, where the benefit of doing so clearly outweighs the potential harm. They suggest that this would allow public bodies to perform their mandates more effectively, would make section 30.1 consistent with the spirit of FIPPA, and would ensure that FIPPA complies with international standards and Canada's international treaty obligations.

**1. Allowing Public Bodies to Effectively Perform Their Mandates**

Members suggest that section 30.1 has detrimentally affected public bodies' ability to effectively provide public services in at least two ways: it has reduced their access to many cloud-based tools, and has hampered the effectiveness of their international operations.

It is a trite observation that information services are becoming steadily more complex and specialized, and are increasingly moving to cloud-based platforms, many of which store information outside Canada. Section 30.1 does not allow public bodies to allow their personal information to be stored or accessed outside Canada – with narrow exceptions – which significantly reduces the ability of public bodies to use technology and services that their counterparts in other jurisdictions take for granted. This trend will only become more pronounced as information services become increasingly multi-jurisdictional. In many cases, we understand that effective Canadian-based alternatives

to these services are simply not available. Lack of choice will, inevitably, require public bodies to accept less effective, often more costly solutions, or to custom-build and support their own applications in-house. The latter course would inevitably be more expensive, as the majority of public bodies would not have the resources dedicated to building these solutions. The latter could also expose public bodies to potential intellectual property lawsuits if their solutions are similar to commercially available solutions, creating additional costs the public body cannot assume or defend.

Members are concerned that the outright prohibition of many of these tools focuses limited public body IT resources on trying to custom-build solutions or adapt Canadian alternatives that are ill-equipped to fill their service delivery needs, rather than finding the best solution that meets key privacy protection requirements. They observe that this can have the perverse effect of forcing public bodies, by operation of law, to use Canadian-based services that are less secure that their foreign-based competitors. We note, in passing, that section 30.1 prevents personal information from being stored outside Canada even if protected using state-of-the-art encryption.

Another issue that members identified is that section 30.1 effectively prohibits public body employees who are resident outside Canada (as opposed to those temporarily traveling outside the country) from accessing or storing personal information for service delivery purposes. This may unreasonably constrain the ability of international offices of some public bodies (such as the BC Trade and Investment Offices, or the foreign

recruitment agents employed by some BC universities) to collect, store or access personal information for service delivery purposes.

**2. "Data Localization"**

While some large foreign data service providers, such as Microsoft, have promised to "localize" their data centres in Canada, this is unlikely to be an effective solution because section 30.1 requires personal information to be accessed as well as stored in Canada. Therefore, some members argue that to be fully compliant with section 30.1, both the data centre service provider and all of the specialized application providers using those data centres would not merely have to move their data storage to Canada, they would also have to set up legal structures to effectively insulate the data in their Canadian operations from their control. Setting up such structures would be complicated, expensive, and not always in the best interest of those companies, who may not have long-term business plans to undertake such endeavors. Some section members believe that most foreign service providers are unlikely to take this step simply to comply with the privacy legislation in British Columbia.

**3. Inconsistency with Spirit of FIPPA**

Some members assert that section 30.1 is inconsistent with the principle of proportionality that animates FIPPA. That is, FIPPA (with the exception of section 30.1) requires public bodies to take all relevant factors into account when deciding on how to disclose and protect personal information.

In terms of disclosure of personal information, FIPPA recognizes that certain disclosures are permissible because they are not an unreasonable invasion of personal privacy. Section 22(1) provides that:

> **Disclosure harmful to personal privacy**
>
> 22 (1) The head of a public body must refuse to disclose personal information to an applicant if the disclosure would be an unreasonable invasion of a third party's personal privacy.

Sections 22(2), (3) and (4) set out criteria that must be used by the public body to decide whether the disclosure of the personal information would constitute an unreasonable invasion of personal privacy.

Some Section members felt that section 30.1 is inconsistent with section 22 because it prohibits public bodies from implementing solutions that would allow access and disclosure outside of Canada of the same personal information that anyone outside of Canada could obtain through an access to information request.

Section 30 of FIPPA requires security arrangements for personal information to be “reasonable”, which implies that public bodies must take into account all relevant factors, including the level of sensitivity of the information, the scope and context and purposes for the collection and use of the information, and the volume of the information.

Section 30 provides:

> 30 A public body must 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.

Again, section 30.1 is inconsistent with section 30. Public bodies are not necessarily able to exercise discretion to make the security arrangements that are reasonable in the circumstances, taking into account such relevant factors as sensitivity and risk of harm. Rather, they may be compelled to accept inferior, more costly security measures within Canada compared to those offered by a service provider outside Canada.

**4. Inconsistency with International Standards**

While some other jurisdictions have laws that impose restrictions on trans-border data flows, these are generally based on the principle of proportionality: that is, they require entities to put security measures in place that are proportional to the risk of storage of personal information outside Canada. Section 30.1 of FIPPA is almost unique in that it does not permit public bodies to balance risks in any way.

For example, the European Union ("EU")'s data protection regime is based on the principle of proportionality. It has designated a list of countries (including Canada) that have privacy regimes they deem to provide an adequate level of protection to permit the storage of the personal information of EU citizens. It is true that the EU courts and data protection authorities have long had a special concern about the privacy protection

practices of the United States, and the EU Court of Justice court has recently struck down the “Safe Harbour” provisions that allowed EU companies to store data in the United States. However, in that case the EU court remitted the matter to the Irish privacy regulator with instructions to weigh the “adequacy of protection” in view of the security protocols in place. It is this proportional, evidence-based approach that is strikingly absent in section 30.1.

British Columbia’s near-absolute ban on international data flows is also at variance with international protocols and treaties that mandate a proportional response to privacy concerns in these cases.

For example, sections 17 and 18 of the OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data authorize reasonable restrictions in view of the nature of the data and the level of protection of the other country:

> 17. A Member country should refrain from restricting transborder flows of personal data between itself and another Member country except where the latter does not yet substantially observe these Guidelines or where the re-export of such data would circumvent its domestic privacy legislation. A Member country may also impose restrictions in respect of certain categories of personal data for which its domestic privacy legislation includes specific regulations in view of the nature of those data and for which the other Member country provides no equivalent protection.

The OECD guidelines also speak against the creation or propagation of any law that would impede or frustrate Member obligations:

> 18. Member countries should avoid developing laws, policies and practices in the name of the protection of privacy and individual liberties, which would create obstacles to transborder flows of personal data that would exceed requirements for such protection.

Another example is the Trans-Pacific Partnership (TPP), which has enshrined the principle of proportionality in Article 14.13:

> **Article 14.13: Location of Computing Facilities**
>
> 1. The Parties recognize that each Party may have its own regulatory requirements regarding the use of computing facilities, including requirements that seek to ensure the security and confidentiality of communications.
>
> 2. No Party shall require a covered person to use or locate computing facilities in that Party's territory as a condition for conducting business in that territory.
>
> 3. Nothing in this Article shall prevent a Party from adopting or maintaining measures inconsistent with paragraph 2 to achieve a legitimate public policy objective, provided that the measure:

(a) is not applied in a manner which would constitute a means of arbitrary or unjustifiable discrimination or a disguised restriction on trade; and

(b) does not impose restrictions on the use or location of computing facilities greater than are required to achieve the objective.

The above Article of the TPP only allows the parties to impose restrictions regarding the location of computing facilities where the restrictions are to achieve a “legitimate public policy objective”, are not “arbitrary or unjustifiable” and are not “greater than are required to achieve the objective.”

Some members have expressed concern that section 30.1 may not comply with any of these requirements, because it prevents public bodies from exercising any discretion when it comes to foreign storage or access. This may make actions taken for the purpose of complying with section 30.1 vulnerable to a challenge from another party under the dispute settlement provisions of TPP.

**Proposal 2**

FIPPA could be amended to authorize public bodies to allow foreign access/storage of personal information in their custody or under their control where sufficient security measures are in place, by amending the Act to add new subsection 33.1(1)(p.1), which would read as follows:

(p.1) the disclosure

(i) is necessary for effecting service delivery using systems or equipment outside Canada that are significantly more functional and/or cost-effective than systems or equipment available for use in Canada, and

(ii) provides security arrangements against such risks as unauthorized access, collection, use, disclosure or disposal that are reasonable having regard to the type, volume and sensitivity of the information, the contractual safeguards in place with the foreign service provider, and the privacy regime in place in the foreign jurisdiction.

To minimize the conflict between subsections 30.1 and the proposed amendment to section 33.1(1), the members also proposed adding a new subsection 30.1(d), which would read as follows:

(d) if it was disclosed under section 33.1(1)(p.1).

Ministries are already subject to an adequate level of oversight, because, under section 69(5.1), they are required to conduct privacy impact assessments for a new enactment, system, project, program or activity, and submit this to the minister for review and comment. Failure to consult may result in the non-acceptance of the proposed solution or enactment, thereby frustrating service delivery and the ministry's mandate.

However, for public bodies that are not ministries, these members recommended that additional oversight by the Commissioner be required for foreign access or disclosure by amending section 69(5.4) as follows:

> (5.4) The head of a public body that is not a ministry, with respect to a proposed system, project, program or activity, must submit, during the development of the proposed system, project, program or activity, the privacy impact assessment, if it addresses a common or integrated program or activity, a data-linking initiative or storage or access to personal information outside Canada, to the commissioner for the commissioner's review and comment.

## B. APPLICATION OF FIPPA TO WHOLLY-OWNED SUBSIDIARIES OF PUBLIC BODIES

In a recent submission to the Special Committee, the Information and Privacy Commissioner advised that there is no sound policy reason why corporations or other agencies created by public bodies should not fall under FIPPA. Her recommendation was to "amend FIPPA to move paragraph (n) of the definition of "local government body" into the definition of "public body" in Schedule 1, so that entities such as subsidiaries of educational bodies and the BCACP fall within the scope of FIPPA." Paragraph (n) reads:

> (n) any board, committee, commission, panel, agency or corporation that is created or owned by a body referred to in paragraphs (a) to (m) and all the members or officers of which are appointed or chosen by or under the authority of that body, (the "Recommended Amendment").

We understand that the Recommended Amendment is intended to address the finding by the BC Supreme Court in *Simon Fraser University v. British Columbia (Information and Privacy Commissioner),* 2009 BCSC 1481 (CanLII) ("Simon Fraser") that public bodies' wholly-owned subsidiaries are not subject to FIPPA unless one can apply the stringent legal test for "piercing the corporate veil". The Court quoted with approval the formulation of the test set out by the Supreme Court of Canada in *Aluminum Co. of Canada Ltd. v. Toronto,* 1944 CanLII 6 (SCC), [1944] 3 D.L.R. 609 (S.C.C.) at 614:

> The question, then, in each case, apart from formal agency which is not present here, is whether or not the parent company is in fact in such an intimate and immediate domination of the motions of the subordinate company that it can be said that the latter has, in the true sense of the expression, no independent functioning of its own.

We do not take any position on which entities should fall within the scope of the Act. However, if the Legislature wishes to change the current system, it needs to carefully consider these changes to minimize the risk of confusion and unintended consequences. In this regard, some members raised two specific concerns with the Recommended Amendment: how it would apply to unincorporated entities, and corporations owned for investment purposes.

**1. Application to Unincorporated Entities**

To address the implications of the Simon Fraser decision, it is only necessary to make incorporated entities subject to the FIPPA. However, the Recommended Amendment goes much further by including unincorporated entities such as a “board, committee, commission, panel [or] agency”. This is unnecessary because in most if not all of these circumstances, these entities would already fall under the control of that public body, and therefore are already subject to FIPPA. Transforming them all into independent public bodies would not be beneficial, and, as some members observed, could possibly lead to unintended harms.

For example, public bodies have large numbers of committees composed of staff, and occasionally third parties. There is no question that the records produced by these committees fall under the custody or control of the public bodies that created them. Under the proposed definition, however, each of these committees would be transformed into an independent public body, which would have a duty to comply with

the manifold responsibilities imposed by FIPPA, such as appointing a Head, responding to access requests, and performing Privacy Impact Assessments. This multitude of new public bodies would have to be trained and resourced to perform these tasks, which would impose a large new administrative burden without any benefit to the public interest.

**2. Application to Corporations Owned for Investment Purposes**

Another question raised by the Recommended Amendment is the appropriate ownership threshold for corporations owned purely for investment purposes. Many public bodies hold shares of corporations in employee pension plans. The question is whether these corporations, which are only owned for investment reasons, should be caught under the scope of the Recommended Amendment.

The proposed definition creates a two-part test: the entity must be “created or owned by” a public body, and “all the members or officers of the entity” must be “appointed or chosen by or under the authority of the public body”. Under this test, the extent of the public body’s ownership interest is unspecified. Would it be sufficient for the public body to hold a controlling interest in the corporation? Some members suggested that this would raise the possibility of corporations gaining the status of public bodies on one day and losing it the next, depending on whether a public body owns more or less than 50% of their shares. Members also raised questions as to the time required to bring such corporations into compliance with FIPPA (especially in these “in-and-out-of-FIPPA” circumstances), and how to comply with the restrictions imposed by section 30.1 on

foreign storage of personal information if the subsidiary corporation is not located in Canada. In the absence of a fulsome consideration of the types of entities which might become subject to such an amendment, such changes could create real and complex unintended consequences.

**Proposal 3**

Therefore, if the Committee decides that wholly-owned subsidiaries of public bodies should fall under the scope of FIPPA, any amendments intended to capture subsidiary agencies of public bodies should apply to only to legal entities, rather than including boards or committee or panels or the like; but in any event should not apply to corporations owned exclusively for investment purposes.

## C. CONDUCTING EMPLOYMENT INVESTIGATIONS

In the wake of Investigation Report F15-01, some members have given fresh consideration to the distinction between direct and indirect collection of personal information in the context of employment investigations. They have observed that there are different notification requirements for direct and indirect collection of personal information, which may compromise the effectiveness or fairness of such investigations.

Public bodies, like their counterparts in the private sector, require legal authority to investigate allegations of inappropriate conduct by their employees. For example, a public body may investigate complaints or concerns by interviewing coworkers,

reviewing paper or electronic files or logs of the activities of the employee, or may collect evidence through direct observation of the employee.

In some cases, these are lengthy or complex investigations that need to be conducted in secret to avoid tipping off the individual being investigated, which could allow them to destroy or tamper with incriminating evidence.

Currently, however, FIPPA restricts public bodies' ability to conduct confidential investigations. While it allows them to collect personal information indirectly without notifying the employee, it does not allow them to directly collect such information without notification. Some Section members felt that this is a strange and arbitrary distinction, with no public policy rationale, and possible negative consequences for public bodies.

**1. Difference between Direct and Indirect Collection**

According to the Information and Privacy Commissioner, "Information is collected directly from an individual when the disclosure to the public body occurs as a result of the individual's own activities. Information is collected indirectly when it is obtained from some source other than the individual concerned." Order F07-18, *University of British Columbia (Re),* 2007 CanLII 42407 (BC IPC) at para. 104 ("Order F07-18").

In Order F07-18, the Commissioner found that the viewing of an employee's internet log reports constitutes "direct" collection of information because these records are created by the individual's own activities. The Commissioner made a similar finding in

Investigation Report F15-01, *Use of Employee Monitoring Software by the District of Saanich*, 2015 BCIPC No. 15. It follows from this that collecting emails from an individual's email server, viewing their social media postings or filming them using a covert camera are all examples of direct, not indirect, collection of their personal information.

The distinction between direct and indirect collection of personal information is relevant to the present discussion because FIPPA requires public bodies to notify employees in an investigation when they directly collect their personal information, but not when they indirectly collect the information.

**2. Notification Requirements for Indirect Collection**

Section 27(1)(f) of FIPPA allows public sector employers to indirectly collect personal information about an employee for the purposes of "managing or terminating an employment relationship".

When information is indirectly collected under section 27(1)(f), section 27(4) exempts the public body from the requirement to notify the employee under the following circumstances:

> 27(4) A public body must notify an employee, other than a service provider, that it will be collecting personal information under subsection (1) (f) unless it is reasonable to expect that the notification would compromise
>
> (a) the availability or the accuracy of the information, or

(b) an investigation or a proceeding related to the employment of the employee.

**3. Notification Requirements for Direct Collection**

However, as explained above, section 27(4) only applies to indirect collection of information about an employee, which is essentially limited to interviewing witnesses or complainants. When a public body employer collects information directly from the employee, section 27(4) does not apply. This means that public bodies must always notify their employees when they are directly collecting their personal information, even if doing so will compromise the availability or the accuracy of the information, or an investigation or a proceeding related to the employment of the employee.

Under section 27(3) of FIPPA, the notification must include "(a) the purpose for collecting it, (b) the legal authority for collecting it, and (c) the title, business address and business telephone number of an officer or employee of the public body who can answer the individual's questions about the collection."

**4. Impact of the Differing Notification Requirements**

This strange inconsistency in notification requirements depending on whether the collection is direct or indirect – which does not exist in the Personal Information Protection Act -- can make it impossible for public bodies to conduct an effective investigation. For example, when investigating an allegation of serious wrongdoing by an employee, the employer does not have to notify the employee before it interviews

witnesses (because this is indirect collection) but it does have to notify the employee that it will be reviewing his internet logs (because this is direct collection) – even if by doing so, the employee will have an opportunity to tamper with the evidence and thereby compromise the availability or accuracy of the information. We can only conclude that this was a drafting error.

**Proposal 4**

These Section members propose that FIPPA be amended to permit a public body to not notify the employee that it is collecting their personal information, either indirectly or directly, where it is reasonable to expect that doing so would compromise (a) the availability or the accuracy of the information, or (b) an investigation or a proceeding related to the employment of the employee.

## D. CLARIFICATION OF LANGUAGE PERMITTING ACCESS TO DOCUMENTS OTHERWISE PROTECTED BY SOLICITOR-CLIENT PRIVILEGE

Some Section members are concerned that the combined impact of some recent decisions of the Information and Privacy Commissioner may weaken the scope of the FIPPA's protection of information that is subject to solicitor-client privilege. In particular, they note that in the last year, section 25, the public interest disclosure provision, has been re-interpreted to apply more broadly than before.[1]

[1] See Investigation Report F15-02 *Review of the Mount Polley Mine Tailings Pond Failure and Public Interest Disclosure by Public Bodies.*

2 Leave to appeal to the SCC allowed *Information and Privacy Commissioner of Alberta v. Board of Governors of*

The newly articulated duty emerging from Investigation Report F15-02 is: “public bodies must disclose information pursuant to s. 25(1)(b) where a disinterested and reasonable observer, knowing what the information is and knowing all of the circumstances, would conclude that disclosure is plainly and obviously in the public interest.”

Members have observed that the reasoning in subsequent Orders suggest that where this test was met, information that is subject to solicitor-client privilege would not be exempt from disclosure in response to a request for access. This has created some confusion and doubt as to the manner in which the duty under s. 25 should be balanced with the long-standing principles undergirding the law of privilege. In other words, it now appears that even where it is proven that the information or the record is subject to solicitor-client privilege, this new broader public interest disclosure duty could arguably trump that protection, and privileged information would have to be disclosed.

The importance of solicitor-client privilege to the proper functioning of the Canadian justice system has been recounted time and again. For instance in *Canada (Privacy Commissioner) v. Blood Tribe Department of Health*, [2008] 2 SCR 574, 2008 SCC 44 (*Blood Tribe)*:

> [9] Solicitor-client privilege is fundamental to the proper functioning of our legal system. The complex of rules and procedures is such that, realistically speaking, it cannot be navigated without a lawyer’s expert advice. It is said that anyone who represents himself or herself has a fool for a client, yet a lawyer’s advice is only as good as the factual information the client provides. Experience shows that people who have a legal problem will often not make a clean breast of the facts to a lawyer without an assurance of confidentiality “as close to absolute as possible”:

> [S]olicitor-client privilege must be as close to absolute as possible to ensure public confidence and retain relevance. As such, it will only yield in certain clearly defined circumstances, and does not involve a balancing of interests on a case-by-case basis.
>
> (*R. v. McClure*, [2001] 1 S.C.R. 445, 2001 SCC 14 (CanLII), at para. 35, quoted with approval in *Lavallee, Rackel & Heintz v. Canada (Attorney General),* [2002] 3 S.C.R. 209, 2002 SCC 61 (CanLII), at para. 36.)

> It is in the public interest that this free flow of legal advice be encouraged. Without it, access to justice and the quality of justice in this country would be severely compromised. The privilege belongs to the client not the lawyer. In *Andrews v. Law Society of British Columbia*, 1989 CanLII 2 (SCC), [1989] 1 S.C.R. 143, at p. 188, McIntyre J. affirmed yet again that the Court will not permit a solicitor to disclose a client's confidence. [underlining added].

There must be clear, express statutory language in order for a statutory body to have access to information protected by solicitor-client privilege: *Blood Tribe*. Recently, the Alberta Court of Appeal in *University of Calgary v. JR*, 2015 ABCA 118[2] has clarified what clear and express statutory language means:

> [26] The presumption in cases involving solicitor-client privilege is that all information protected by solicitor-client privilege lies beyond the reach of others, including the state. In other words, the analytical starting-point is that the state – including an official of the administrative state such as the Commissioner – is not, as a matter of fundamental justice, entitled to such information: *Lavallee* at para 24. The question here, then, is whether this Court should understand the Legislature as having, by enacting section 56(3) of FIPPA, displaced that presumption.
>
> …
> [48] These reasons, taken together, describe the rule of strict construction as demanding ofstatutory language the highest degree of clarity, explicitness and specificity in order to support a conclusion that it was intended to authorize infringements of solicitor-client privilege. That is, it requires language which is absolutely clear, such that the underlying legislative intent is completely explicit. **This requires specific reference to solicitor-client privilege.** Departing from this stricture would undermine the rationale for the rule of strict construction of

2 Leave to appeal to the SCC allowed *Information and Privacy Commissioner of Alberta v. Board of Governors of the University of Calgary*, 2015 CanLII 69443 (SCC) – October 29, 2015.

> statutory language in such cases – being solicitor-client privilege's central and (among all privileges recognized in law) unique importance to the proper functioning of the legal system. It is "extremely important, indeed constitutionally protected … and can be lost only in narrowly defined circumstances": *Piikani Nation v Kostic*, 2015 ABCA 60 (CanLII) at para 1,[2015] AJ No 172 (QL). Those narrowly defined circumstances, so far as statutory abrogations of solicitor-client privilege are concerned, are not satisfied by statutory language which might, owing to its generality, reasonably bear more than one interpretation. Otherwise, there remains a risk that legislators did not intend that infringement. In other words, the driving concern for courts in such cases is whether the posited infringement of solicitor-client privilege was clearly intended. [emphasis added]

Unlike the Alberta Privacy Commissioner in *University of Calgary*, the FIPPA does have clear and specific reference to solicitor-client privilege, in section 44, under which the B.C. Privacy Commissioner is empowered to compel the production of records, even where solicitor-client privilege is claimed:

> s. 44(3) Despite any other enactment or any privilege of the law of evidence, a public body must produce to the commissioner within 10 days any record or a copy of any record required under subsection (1).

The privilege is protected by operation of section 44(2.1) of FIPPA, which provides that production of privileged records ***to the commissioner*** does not breach the privilege:

> s. 44(2.1) If a person discloses a record that is subject to solicitor client privilege to the commissioner at the request of the commissioner, or under subsection (1) [power of the Commissioner to order the production of a record to the Commissioner], the solicitor client privilege of the record is not affected by the disclosure.

These members noted that the privilege is protected only when the records are disclosed to the commissioner. For obvious reasons, it couldn't be protected where the records are disclosed more broadly.

Given that s. 25(2) overrides any other provision of the Act, the risk identified by some of our members is that a broadened interpretation of section 25 may inappropriately capture records previously protected under section 14, which protects information subject to solicitor-client privilege.

**1. Section 14 of FIPPA: Solicitor-Client Privilege**

Under section 14 of FIPPA, a public body may refuse disclosure of information that is subject to solicitor-client privilege. This right is discretionary, and is generally exercised in consultation with the client whose privilege is at issue. Of course, the privilege belongs to the client and they may choose not to waive the privilege.

A subset of solicitor-client privilege is litigation privilege. Litigation privilege generally protects communications between a lawyer and third parties where litigation is reasonably contemplated or ongoing. It protects the communication a lawyer may need to engage in with others (example expert witnesses) who may be of assistance to his or her client's case "without adversarial interference and without fear of premature disclosure": *Blank v. Canada (Minister of Justice)* 2006 SCC 39, [2006] 2 SCR 319 at paragraph 27. The privilege ends, when the litigation ends: *Blank.* Section 14 of FIPPA also includes protection of records where litigation privilege is claimed: *College of*

*Physicians of B.C. v. British Columbia (Information and Privacy Commissioner),* 2002 BCCA 665 at paragraph 26.

The B.C. Privacy Commissioner has recognized the right of public bodies to claim solicitor-client privilege, litigation privilege and common interest privilege:[3]

- Solicitor-Client Privilege: *The Board of Education of School District 71 (Comox Valley)*, *Order F15-67* (December 3, 2015);

- Litigation Privilege: *Ministry of Health* Order *F15-41* (August 21, 2015); and

- Common Interest Privilege: *Victoria Police Department* Order *F15-61* (November 10, 2015).

**2. Section 57 of FIPPA: Proving the Right to Refuse Disclosure**

Under Section 57 of FIPPA the burden of proof lies on the public body or third party to establish that an application has no right of access to a record, including proving that section 14 applies to exempt the record from disclosure because the record contains solicitor-client privileged communications. This is generally demonstrated by affidavit material filed as evidence by the public body or third party. The adjudicator must also review the records, as was the case in, for example, *Ministry of Health Order F15-41.*

3 A form of solicitor-client privilege where many litigants have shared legal advice or communications covered by "litigation privilege" due to a common interest in the advice.

**3. Section 25**

Section 25 of FIPPA provides:

> 25 (1) Whether or not a request for access is made, the head of a public body must, without delay, disclose to the public, to an affected group of people or to an applicant, information
>
> > (a) about a risk of significant harm to the environment or to the health or safety of the public or a group of people, or
> >
> > (b) the disclosure of which is, for any other reason, clearly in the public interest.
>
> (2) Subsection (1) applies despite any other provision of this Act.
>
> (3) Before disclosing information under subsection (1), the head of a public body must, if practicable, notify
>
> > (a) any third party to whom the information relates, and
> >
> > (b) the commissioner.
>
> (4) If it is not practicable to comply with subsection (3), the head of the public body must mail a notice of disclosure in the prescribed form
>
> > (a) to the last known address of the third party, and
> >
> > (b) to the commissioner.

The test enunciated in Investigation Report F15-02 was applied in *Ministry of Health Order F15-64*, and the adjudicator concluded that it was not met. Then the adjudicator considered whether the information was protected by s. 14, and found that it was.

Some members have suggested that the this analysis was done in the wrong order and that the section 14 analysis should be done first, so as to ensure that, if the privilege was found to apply, *that fact would be considered* when considering whether the new section 25 test of "knowing what the information is and knowing all of the circumstances."

In other words, although section 25 will apply despite any other provision of the Act, the fact that another provision of the Act applies should be a factor to consider when weighing whether the public interest militates in favour of disclosure.

It is unsurprising that lawyers would feel so strongly about the importance of protecting this fundamental principle. As the Supreme Court of Canada said in *Blood Tribe* at paragraph 9:

> [9] Solicitor-client privilege is fundamental to the proper functioning of our legal system. The complex of rules and procedures is such that, realistically speaking, it cannot be navigated without a lawyer's expert advice. It is said that anyone who represents himself or herself has a fool for a client, yet a lawyer's advice is only as good as the factual information the client provides. Experience shows that people who have a legal problem will often not make a clean breast of the facts to a lawyer without an assurance of confidentiality "as close to absolute as possible":
>
> > [S]olicitor-client privilege must be as close to absolute as possible to ensure public confidence and retain relevance. <u>As such, it will only yield in certain clearly defined circumstances, and does not involve a balancing of interests on a case-by-case basis.</u>
>
> (*R. v. McClure*, [2001] 1 S.C.R. 445, 2001 SCC 14, at para. 35, quoted with approval in *Lavallee, Rackel & Heintz v. Canada (Attorney General*), [2002] 3 S.C.R. 209, 2002 SCC 61, at para. 36.)[underline added]

Put another way, protecting solicitor-client privilege is in the public interest because the privilege is fundamental to the functioning of our legal system and doing so ensures public confidence in administration of justice.

**Proposal 5**

Section members agreed on the importance of protecting solicitor-client privilege. However, there was no agreement as to the best way of doing so.

Some members suggested amending s. 14 to explicitly exempt records that are privileged from s. 25 or exempting privileged records from the scope of the Act under section 3. Others urged this Committee to amend the Act to include a list of factors to be considered when determining the public interest, and that these factors should include whether the record is protected by another section of the Act and whether the record is protected by solicitor-client privilege.

## E. MANDATORY BREACH NOTIFICATION

FIPPA currently does not have sections providing guidance on mandatory breach notification. The effect is that public bodies are often confused as to their duties when managing breaches. Specifically, the following issues apply:

- Does the public body have a duty to notify the OIPC of breaches?

- Does the public body have a duty to notify the public and stakeholders of breaches?

- If so, what is the definition or test of breach that must be met in order to trigger these duties?

- What is the scope and scale of personal information compromised that would trigger the duty?

In Canada, private-sector mandatory breach notification is already required for organizations subject to the federal *Personal Information Protection and Electronic Documents Act* (PIPEDA) through amendments made to PIPEDA under the *Digital Privacy Act*.

Some members submit that FIPPA should be amended to include requirements on public bodies to determine if a breach of personal information should be disclosed, whom to notify, and the time within which they must provide notification. These members note that although this is part of best practice in breach and incident response, mandatory breach notification should not be construed as a complete replacement of incident response work flow. They note that such an amendment would also ensure that BC public bodies comply with international standards such as the Organisation for Economic Co-operation and Development Guidelines.

**1. Significant Harm**

Mandatory breach notification first became law in the Alberta private sector in 2010, with the introduction of their updated *Personal Information Protection Act*, SA 2003, c. P-6.5. This requires private-sector entities to disclose breaches so long as the information that was compromised was collected by them and entrusted to their care, irrespective of the information being compromised by a third party in a related transaction. In particular, the Alberta OIPC released Orders P2011-ND-011 and P2011-ND-012, in which they reviewed breaches the occurred when Best Buy and Air Miles provided customer personal information to the third party marketing firm Epsilon, resulting in more than 50 million customer personal information being compromised. Although the third party suffered the breach, the obligation was still on Best Buy and Air Miles as the entities collecting the personal information to advise their customers of the breach. In particular, these Orders discussed factors of "significant harm", including taking into account the following:

> [T]he magnitude of the breach, that is the number of affected individuals, the maliciousness of the breach including whether there are indications personal information was misappropriated for nefarious purposes, the sensitivity of the information and the harm that may result.

The sheer volume of the breach and its far-reaching effects necessitated breach notification. Although public bodies may not have the same number of customers as in the Best Buy/Air Miles situation, they hold such sensitive information as health care details, social insurance number, police records and other sensitive information that, if compromised, would result in mass identity theft. In worst-case scenarios, this would hamper citizens to the point where identity thieves could use their personal information

to open credit cards and bank accounts, and access services and other benefits under those false identities which would detrimentally affect the affected individuals' credit ratings and health records, resulting in the ruination of their medical and financial health and, at worst, resulting in criminal charges being levied upon unsuspecting individuals. Public bodies collect and hold large amounts of personal information which, if compromised, could result in harm to citizens and a loss of confidence in the government and public entities in general.

The mandatory breach requirement has, since June 23, 2015, become applicable in the private sector under the newly proposed sections 10.1, 10.2 and 10.3 of PIPEDA (*Digital Privacy Act*), SC 2000, c. 5. Although those sections have not yet come into force, these requirements will eventually become standardized while also empowering the commissioners to investigate breaches.

Some members noted that the mandatory breach notification requirements are anticipated to mirror those in the EU, particularly the General Data Protection Regulation (GDPR) and the Network Information Security (NIS) directive, both of which regulate the notice obligations for entities conducting business in the EU. Although both the GDPR and NIS directives are currently in the making, their principles will be based on the Data Protection Directive (Directive 95/46/EC) that protects the rights of individuals' personal data when used by organizations. Failure to comply or provide similar protection in the law may lead to results such as the revocation of the EU Safe Harbour agreement between the US and the EU, substantially jeopardizing the

movement of personal information and business initiatives protecting and processing the same between the US and the EU.

**Proposal 6**

These members propose the addition of mandatory breach notification in two parts of FIPPA:

- The obligation on the public entity's requirement to provide notice to stakeholders should be part of **Part 3, Division 4**, under a new section to be numbered **36.2**;

- The powers of the OIPC to investigate any breaches emanating from the proposed s. 36.2 should be expanded under s. 44, the "powers of commissioner in conducting investigations, audits or inquiries", under the new section to be numbered **44.3**; and

- Further details on the form of notification should be added to a new **Schedule 4**.

The wording at s. 36.2 should be similar to Alberta's PIPA s. 34.1, which currently reads as follows:

> (1) An organization having personal information under its control must, without unreasonable delay, provide notice to the Commissioner of any incident involving the loss of or unauthorized access to or disclosure of the 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.

(2) A notice to the Commissioner under subsection (1) must include the information prescribed by the regulations.

The interpretation of “without unreasonable delay” would initially be discretionary and evaluated on a case-by-case basis, but public bodies could look to existing jurisprudence (interpreting the Alberta PIPA or private sector privacy laws) for guidance.

The wording at s. **44.3** could be similar to Alberta’s PIPA s. 37.1:

**44.3(1)** Where an organization suffers a loss of or unauthorized access to or disclosure of personal information that the organization is required to provide notice of under section 36.2, the Commissioner may require the organization to notify individuals to whom there is a real risk of significant harm as a result of the loss or unauthorized access or disclosure

(a) in a form and manner prescribed by the regulations, and

(b) within a time period determined by the Commissioner.

**(2)** If the Commissioner requires an organization to notify individuals under subsection (1), the Commissioner may require the organization to satisfy any

terms or conditions that the Commissioner considers appropriate in addition to the requirements under subsection (1).

**(3)** The Commissioner must establish an expedited process for determining whether to require an organization to notify individuals under subsection (1) in circumstances where the real risk of significant harm to an individual as a result of the loss or unauthorized access or disclosure is obvious and immediate.

**(4)** The Commissioner may require an organization to provide any additional information that the Commissioner considers necessary to determine whether to require the organization

(a) to notify individuals under subsection (1), or

(b) to satisfy terms and conditions under subsection (2).

**(5)** An organization must comply with a requirement

(a) to provide additional information under subsection (4),

(b) to notify individuals under subsection (1), or

(c) to satisfy terms and conditions under subsection (2).

**(6)** The Commissioner has exclusive jurisdiction to require an organization

(a) to provide additional information under subsection (4),

(b) to notify individuals under subsection (1), or

(c) to satisfy terms or conditions under subsection (2).

**(7)** Nothing in this section is to be construed so as to restrict an organization's ability to notify individuals on its own initiative of the loss of or unauthorized access to or disclosure of personal information.

Both of the two draft sections make reference to "regulations". Specifically, the form and content of the notices to the public or stakeholders in the events of breaches should also be part of the regulations, with the most logical place for this in a new **Schedule 4** to FIPPA. The proposed **Schedule 4** could be very similar to the Alberta PIPA, which currently reads as follows:

**Schedule 4**

**Notification of Loss of or Unauthorized Access to or Disclosure of Personal Information**

**Notice to the Commissioner**

**1** A notice provided by an organization to the Commissioner under section 36.2(1) of the Act must be in writing and include the following information:

(a) a description of the circumstances of the loss or unauthorized access or disclosure;

(b) the date on which or time period during which the loss or unauthorized access or disclosure occurred;

(c) a description of the personal information involved in the loss or unauthorized access or disclosure;

(d) an assessment of the risk of harm to individuals as a result of the loss or unauthorized access or disclosure;

(e) an estimate of the number of individuals to whom there is a real risk of significant harm as a result of the loss or unauthorized access or disclosure;

(f) a description of any steps the organization has taken to reduce the risk of harm to individuals;

(g) a description of any steps the organization has taken to notify individuals of the loss or unauthorized access or disclosure;

(h) the name of and contact information for a person who can answer, on behalf of the organization, the Commissioner's questions about the loss or unauthorized access or disclosure.

**Notification to individuals**

**2 (1)** Where an organization is required under section 36.2 of the Act to notify an individual to whom there is a real risk of significant harm as a result of a loss of or unauthorized access to or disclosure of personal information, the notification must

(a) be given directly to the individual, and

(b) include

(i) a description of the circumstances of the loss or unauthorized access or disclosure,

(ii) the date on which or time period during which the loss or unauthorized access or disclosure occurred,

(iii) a description of the personal information involved in the loss or unauthorized access or disclosure,

(iv) a description of any steps the organization has taken to reduce the risk of harm, and

(v) contact information for a person who can answer, on behalf of the organization, questions about the loss or unauthorized access or disclosure.

(2) Notwithstanding subsection (1)(a), where an organization is required to notify an individual under section 36.2 of the Act, the notification may be given to the individual indirectly if the Commissioner determines that direct notification would be unreasonable in the circumstances.

## F. THE DUTY TO DOCUMENT

There was no consensus among our members on the duty to document. However, we can say that everyone has a keen interest in understanding the potential scope of any such obligation. While there may not be consensus on how best to handle the issue, the findings in the recent 2015 OIPC "Access Denied" report about an apparent culture of oral governance on the part of the provincial government are a real concern for many of the members. The imposition of a duty to document should not be considered in

isolation from issues relating to the entire life cycle (classification, storage, security, retention and destruction) of records that are created and that become subject to FIPPA. Former Commissioner Loukidelis refers to this in his December 2015 report to government as “a culture of proper records management”. In particular, consideration must be given to the fact that the Information Management Act applies only to a subset of the public bodies that are regulated by FIPPA. Many public bodies in the broader public service have little or no legislative guidance to assist with managing the life cycle of records, and have inadequate resources to develop something independently. This was recognized by the legislative review committee in Newfoundland in its 2014 review of that province’s access to information legislation, resulting in a recommendation that “adequate resources be provided to public bodies served by the Office of the Chief Information Officer, so that there is consistency in the performance of information management systems”.

The duty to document has, in various places, been referenced as applying to “key” or “non-trivial” decisions. We query whether these terms provide sufficient guidance to all public bodies, particularly those that are substantially operational in nature (the regional health authorities are a good example, as is BC Ferries, British Columbia Lottery Corporation, etc.) about what types of decisions must be documented. Are these to be interpreted as key/non-trivial decisions of the public body corporate (e.g. a particular policy direction?), or would these include the many important day-to-day operational decisions that occur in many public bodies?

All in all, as per former Commissioner Loukidelis' recommendation in his report, this issue merits careful study prior to being implemented (a) within government, and (b) more importantly, in a broad-based way to all public bodies in the broader public service. Stakeholder consultation with the broader public service, as well as citizens generally, would be beneficial to understanding the concerns public bodies have about the impact of imposing such a duty, and whether these concerns amount to more than simply an irrational fear that their operations will grind to a halt.

Is FIPPA the most appropriate statutory vehicle through which to impose a duty to document, or should such a duty be embedded in legislation and/or policy that deals with information management more generally?

Finally, what are the most appropriate consequences in the face of such a duty for non-compliance? Is the OIPC adequately resourced to manage the investigation of such complaints? Should the mandate of the OIPC be expanded in this way (which connects to the issue of whether FIPPA is the appropriate statutory vehicle through which to impose this type of duty).

## CONCLUSION

We would be pleased to discuss our submissions further with 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 important review.

Communications in this regard can be directed to:

**RITCHIE PO**

Co-Chair, CBABC Freedom of Information and Privacy Law Section

Tel.: 778-875-1689

Email: ritchie.po@telus.com

**SARA ANN LEVINE, Q.C.**

Co-Chair, CBABC Freedom of Information and Privacy Law Section

Tel.: (604) 877-1057

Email: slevine@alliancelex.com

## LIST OF RECOMMENDATIONS

**Proposal 1**

For the reasons discussed below, some Section members recommended that FIPPA be amended to give public bodies discretion to store or access personal information outside Canada under limited circumstances, where the benefit of doing so clearly outweighs the potential harm. They suggest that this would allow public bodies to perform their mandates more effectively, would make section 30.1 consistent with the spirit of FIPPA, and would ensure that FIPPA complies with international standards and Canada's international treaty obligations.

**Proposal 2**

FIPPA could be amended to authorize public bodies to allow foreign access/storage of personal information in their custody or under their control where sufficient security measures are in place, by amending the Act to add new subsection 33.1(1)(p.1), which would read as follows:

(p.1) the disclosure

(i) is necessary for effecting service delivery using systems or equipment outside Canada that are significantly more functional and/or cost-effective than systems or equipment available for use in Canada, and

(ii) provides security arrangements against such risks as unauthorized access, collection, use, disclosure or disposal that are reasonable having

regard to the type, volume and sensitivity of the information, the contractual safeguards in place with the foreign service provider, and the privacy regime in place in the foreign jurisdiction.

To minimize the conflict between subsections 30.1 and the proposed amendment to section 33.1(1), the members also proposed adding a new subsection 30.1(d), which would read as follows:

(d) if it was disclosed under section 33.1(1)(p.1).

Ministries are already subject to an adequate level of oversight, because, under section 69(5.1), they are required to conduct privacy impact assessments for a new enactment, system, project, program or activity, and submit this to the minister for review and comment. Failure to consult may result in the non-acceptance of the proposed solution or enactment, thereby frustrating service delivery and the ministry's mandate.

However, for public bodies that are not ministries, these members recommended that additional oversight by the Commissioner be required for foreign access or disclosure by amending section 69(5.4) as follows:

(5.4) The head of a public body that is not a ministry, with respect to a proposed system, project, program or activity, must submit, during the development of the proposed system, project, program or activity, the privacy impact assessment, if it addresses a common or integrated program or activity, a data-linking initiative

or storage or access to personal information outside Canada, to the commissioner for the commissioner's review and comment.

**Proposal 3**

Therefore, any amendments intended to capture subsidiary agencies of public bodies should apply to only to legal entities, rather than including boards or committee or panels or the like; but in any event should not apply to corporations owned exclusively for investment purposes.

**Proposal 4**

These Section members propose that FIPPA be amended to permit a public body to not notify the employee that it is collecting their personal information, either indirectly or directly, where it is reasonable to expect that doing so would compromise (a) the availability or the accuracy of the information, or (b) an investigation or a proceeding related to the employment of the employee.

**Proposal 5**

Section members agreed on the importance of protecting solicitor-client privilege. However, there was no agreement as to the best way of doing so.

Some members suggested amending s. 14 to explicitly exempt records that are privileged from s. 25 or exempting privileged records from the scope of the Act under section 3. Others urged this Committee to amend the Act to include a list of factors to be considered when determining the public interest, and that these factors should include

whether the record is protected by another section of the Act and whether the record is protected by solicitor-client privilege.

**Proposal 6**

These members propose the addition of mandatory breach notification in two parts of FIPPA:

- The obligation on the public entity's requirement to provide notice to stakeholders should be part of **Part 3, Division 4**, under a new section to be numbered **36.2**;

- The powers of the OIPC to investigate any breaches emanating from the proposed s. 36.2 should be expanded under s. 44, the "powers of commissioner in conducting investigations, audits or inquiries", under the new section to be numbered **44.3**; and

- Further details on the form of notification should be added to a new **Schedule 4**.

The wording at s. 36.2 should be similar to Alberta's PIPA s. 34.1, which currently reads as follows:

> (1) An organization having personal information under its control must, without unreasonable delay, provide notice to the Commissioner of any incident involving the loss of or unauthorized access to or disclosure of the 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.

(2) A notice to the Commissioner under subsection (1) must include the information prescribed by the regulations.

The interpretation of “without unreasonable delay” would initially be discretionary and evaluated on a case-by-case basis, but public bodies could look to existing jurisprudence (interpreting the Alberta PIPA or private sector privacy laws) for guidance.

The wording at s. **44.3** could be similar to Alberta’s PIPA s. 37.1:

**44.3(1)** Where an organization suffers a loss of or unauthorized access to or disclosure of personal information that the organization is required to provide notice of under section 36.2, the Commissioner may require the organization to notify individuals to whom there is a real risk of significant harm as a result of the loss or unauthorized access or disclosure

(a) in a form and manner prescribed by the regulations, and

(b) within a time period determined by the Commissioner.

**(2)** If the Commissioner requires an organization to notify individuals under subsection (1), the Commissioner may require the organization to satisfy any

terms or conditions that the Commissioner considers appropriate in addition to the requirements under subsection (1).

**(3)** The Commissioner must establish an expedited process for determining whether to require an organization to notify individuals under subsection (1) in circumstances where the real risk of significant harm to an individual as a result of the loss or unauthorized access or disclosure is obvious and immediate.

**(4)** The Commissioner may require an organization to provide any additional information that the Commissioner considers necessary to determine whether to require the organization

(a) to notify individuals under subsection (1), or

(b) to satisfy terms and conditions under subsection (2).

**(5)** An organization must comply with a requirement

(a) to provide additional information under subsection (4),

(b) to notify individuals under subsection (1), or

(c) to satisfy terms and conditions under subsection (2).

**(6)** The Commissioner has exclusive jurisdiction to require an organization

(a) to provide additional information under subsection (4),

(b) to notify individuals under subsection (1), or

(c) to satisfy terms or conditions under subsection (2).

**(7)** Nothing in this section is to be construed so as to restrict an organization's ability to notify individuals on its own initiative of the loss of or unauthorized access to or disclosure of personal information.

Both of the two draft sections make reference to "regulations". Specifically, the form and content of the notices to the public or stakeholders in the events of breaches should also be part of the regulations, with the most logical place for this in a new **Schedule 4** to FIPPA. The proposed **Schedule 4** could be very similar to the Alberta PIPA, which currently reads as follows:

**Schedule 4**

**Notification of Loss of or Unauthorized Access to or Disclosure of Personal Information**

**Notice to the Commissioner**

**1** A notice provided by an organization to the Commissioner under section 36.2(1) of the Act must be in writing and include the following information:

(a) a description of the circumstances of the loss or unauthorized access or disclosure;

(b) the date on which or time period during which the loss or unauthorized access or disclosure occurred;

(c) a description of the personal information involved in the loss or unauthorized access or disclosure;

(d) an assessment of the risk of harm to individuals as a result of the loss or unauthorized access or disclosure;

(e) an estimate of the number of individuals to whom there is a real risk of significant harm as a result of the loss or unauthorized access or disclosure;

(f) a description of any steps the organization has taken to reduce the risk of harm to individuals;

(g) a description of any steps the organization has taken to notify individuals of the loss or unauthorized access or disclosure;

(h) the name of and contact information for a person who can answer, on behalf of the organization, the Commissioner's questions about the loss or unauthorized access or disclosure.

**Notification to individuals**

**2 (1)** Where an organization is required under section 36.2 of the Act to notify an individual to whom there is a real risk of significant harm as a result of a loss of or unauthorized access to or disclosure of personal information, the notification must

(a) be given directly to the individual, and

(b) include

(i) a description of the circumstances of the loss or unauthorized access or disclosure,

(ii) the date on which or time period during which the loss or unauthorized access or disclosure occurred,

(iii) a description of the personal information involved in the loss or unauthorized access or disclosure,

(iv) a description of any steps the organization has taken to reduce the risk of harm, and

(v) contact information for a person who can answer, on behalf of the organization, questions about the loss or unauthorized access or disclosure.

(2) Notwithstanding subsection (1)(a), where an organization is required to notify an individual under section 36.2 of the Act, the notification may be given to the individual indirectly if the Commissioner determines that direct notification would be unreasonable in the circumstances.