Office of the
Information &
Privacy Commissioner
for British Columbia

Protecting privacy. Promoting transparency.

STATUTORY REVIEW OF THE FREEDOM OF INFORMATION AND PROTECTION Of PRIVACY ACT

OIPC RESPONSE TO STAKEHOLDER RECOMMENDATIONS TO THE SPECIAL COMMITTEE TO REVIEW THE FREEDOM OF INFORMATION AND PROTECTION OF PRIVACY ACT

Elizabeth Denham
Information and Privacy Commissioner
for British Columbia

March 8, 2016

Contents

INTRODUCTION

The work of the Special Committee, appointed on May 27, 2015, to conduct the 40th Parliament's statutory review of the *Freedom of Information and Protection of Privacy Act* ("FIPPA"), has generated intense interest and engagement.

For more than two decades, FIPPA has been the foundation of the right to access to information and the protection of privacy in British Columbia. This review presents a timely opportunity to carefully examine the Act and consider how it can be improved to make government more accountable and better protect personal privacy.

Without a doubt, the people of BC are concerned about issues that are at the very core of the Act. I was especially encouraged by the volume of submissions supporting a duty to document and oversight over the unauthorized destruction of records. These reforms clearly remain a top priority for British Columbians, and I will address them in detail when I appear before the Committee on March 16, 2016.

I first appeared before you to deliver a *Speech to the Special Committee to Review the Freedom of Information and Protection of Privacy Act* on July 21, 2015 as you began your deliberations. I returned to deliver a second *Speech to the Special Committee to Review the Freedom of Information and Protection of Privacy Act* on November 18, 2015. At that time, I also left you with my office's *Submission to the Special Committee to Review the Freedom of Information and Protection of Privacy Act*.

It is my pleasure now to respond to your request that I provide my views on many of the recommendations that have been made to this Committee. My objective with this submission is to assist the Special Committee in its deliberations. With that in my mind, I have focussed on the areas where my Office has additional information or analysis that may be useful to you in relation to the recommendations. For clarity and ease of reference, I have addressed those recommendations in the order that they arise within FIPPA.

Finally, I would to thank each member of the Special Committee to Review the *Freedom of Information and Protection of Privacy Act* for your work. When I first appeared before you last summer, I noted that a legislative review is a marathon

and not a sprint. Now you are heading into the final lap. The recommendations that you make in these changing times will shape the ways British Columbians will hold their government to account and control their personal information for generations to come.

I remain available to the Special Committee as a resource throughout your review.

March 8, 2016

ORIGINAL SIGNED BY

Elizabeth Denham
Information and Privacy Commissioner for BC

1.0 RECOMMENDATIONS FOR PART 1 OF FIPPA – INTRODUCTORY PROVISIONS

1.1 SECTION 1 – DEFINITIONS

"contact information"

The Insurance Corporation of British Columbia wants FIPPA to authorize public bodies to refuse to disclose contact information to marketers or those seeking that information for personal reasons. To accomplish this, they recommend amending the definition of "contact information" to add a requirement that such information must only be used for business or employment-related purposes.

This amendment is unnecessary as it has already been addressed in OIPC Orders.[1] For example, Order F08-03 states that whether information is "contact information" will depend on the context; if the information is sought for reasons other than a business purpose, then that information is not "contact information" under the Act.[2]

"law enforcement"

The Law Society of British Columbia recommends expanding the definition of "law enforcement" to cover law society proceedings or investigations relating to assessments of character or competence, so that they can refuse to disclose information arising from such investigations or proceedings under s. 15(1)(a) of FIPPA. The Law Society raises two concerns: that it may not be able to refuse disclosures when investigations or proceedings related to character or competence do not have a penalty or sanction attached, and that it may not be able to refuse to disclose information that is received in confidence in relation to these assessments.

This recommendation is unnecessary. Section 15(1)(a) already authorizes the Law Society to refuse disclosing information in relation to investigations or proceedings even if a penalty or sanction does not result. The section refers to investigations or proceedings "that lead or could lead to a penalty or sanction being imposed."[3]

In addition, even if s. 15(1)(a) did not apply, the Law Society's confidentiality concerns are addressed in s. 22 of FIPPA. This section sets out the circumstances that a public body must consider when determining whether a

[1] See Order F05-31, [2005] B.C.I.P.C.D. No. 42 at para. 26 and Order F08-03, [2008] B.C.I.P.C.D. No. 6 at para. 82.
[2] Order F08-03, at para. 82.
[3] FIPPA, Schedule 1, "law enforcement".

disclosure would be harmful to personal privacy. Those considerations balance the interests of the public body, but also of applicants and of third parties. This section *requires* public bodies to consider whether information has been supplied in confidence.[4] It also requires consideration of factors such as whether a third party will be exposed unfairly to harm and whether the personal information is relevant to a fair determination of the applicant's rights.[5]

"public body"

The OIPC has recommended to the Special Committee that the definition of "public body" in FIPPA be amended so that entities such as subsidiaries of educational bodies and the BC Association of Chiefs of Police fall within its scope. A number of organizations that have made submissions to the Committee have also raised this issue.[6] This section includes additional information and legislative models that may assist the Special Committee in determining the appropriate legislative amendments on this matter.

The Act should require an entity to be treated as a public body when it is created or owned by a public body – whether in whole or in part – if it operates with substantial public funds, or benefits or performs a statutory function, public function, or a public service. FIPPA should not contain any loopholes that authorize public bodies to avoid public accountability simply by creating a new entity. An entity that receives public funds, or that plays a public function, should be subject to accountability.

Bringing entities owned and operated by public bodies under FIPPA

In its submission to the Committee, the Canadian Bar Association asked Committee members to limit broadening the definition of "public bodies" to corporate entities, and to exempt corporations owned for investment purposes.

I do not support these recommendations. FIPPA continues to provide a significant loophole that shields these entities from accountability under the Act *unless* they are created by a local government body.

For this reason, I recommended to the Committee that paragraph (n) from the definition of "local government body" be added to the definition of "public body" in Schedule 1. With the addition, the definition would state:

[4] FIPPA, ss. 22(2)(f) and 22(3)(h).
[5] FIPPA, ss. 22(2)(c) and (e).
[6] For example, see submissions to the Committee from the AMS Student Society of UBC Vancouver, BC Freedom of Information and Privacy Association, BC Government and Service Employees Union, the Centre for Law and Democracy, the Canadian Bar Association, Canadian Centre for Policy Alternatives, Canadian Union of Public Employees, British Columbia Division, Canadian Union of Public Employees, Local 116, Integrity BC, and the Ubessey.

"public body" means

(a) a ministry of the government of British Columbia,
(b) an agency, board, commission, corporation, office or other body designated in, or added by regulation to, Schedule 2, or
(c) a local public body,
(d) <u>any board, committee, commission, panel, agency or corporation that is created or owned by a body referred to in paragraphs (a) to (c) and all the members or officers of which are appointed or chosen by or under the authority of that body,</u>

but does not include

(e) the office of a person who is a member or officer of the Legislative Assembly, or
(f) the Court of Appeal, Supreme Court or Provincial Court;[7]

The same language would also remain in the definition of "local government body," which is important for clarity in statutory interpretation.

Adopting this language would ensure the subsidiary entities are held publically accountable. Public bodies should not be able to avoid responsibilities under the Act simply by creating a subsidiary corporation or establishing a panel or agency to carry out a particular function. Each of the listed entities *should* be subject to FIPPA for accountability purposes.

Similarly, corporations should not be exempt from the Act when they are owned for investment purposes; corporations operating under the authority of a public body should also be subject to accountability under FIPPA. In all cases, exceptions under the Act would apply to protect financial or economic interests, business interests of third parties, and personal privacy.[8]

Expand and define criteria for Minister to designate entities as a "public body"

The Centre for Law and Democracy recommended to the Committee that entities that are performing a "public function" should be subject to accountability under FIPPA.

I support this recommendation. Apart from the subsidiary issue, there will be other cases where a question arises as to whether an entity should be considered a public body within the meaning of the Act. An entity could be

[7] The additional language is underlined.
[8] Sections 17, 21, or 22 of FIPPA.

created by more than one public body, or it may be a mix of public and private bodies. An entity could have members or officers that are appointed by more than one public body, or represent a mix of public and private body appointments. It could also be an entity that is clearly carrying out a public function but that does not meet the definition of public body.

For these cases, I am recommending that the criteria in s. 76.1 be expanded to allow the Minister responsible greater latitude to designate an entity as a "public body" when it serves the accountability purpose of FIPPA.

Section 76.1 states:

> 76.1(1) The minister responsible for this Act may, by regulation, amend Schedule 2 to do one or more of the following:
>
> (a) add to it any agency, board, commission, corporation, office or other body
>
> (i) of which any member is appointed by the Lieutenant Governor in Council or a minister,
>
> (ii) of which a controlling interest in the share capital is owned by the government of British Columbia or any of its agencies, or
>
> (iii) that performs functions under an enactment;
>
> (b) designate or change the designation of the head of a public body;
>
> (c) delete from it an agency, board, commission, corporation, office or other body that
>
> (i) no longer exists, or
>
> (ii) no longer meets the criteria established by paragraph (a)

I propose those criteria be expanded to include authorizing the Minister to add to Schedule 2 a body that is performing a public function.

This approach is consistent with the recommendations made by the Information Commissioner of Canada to the federal government that the performance of a public function be considered in any determination of whether an entity is subject to the *Access to Information Act*.[9]

[9] See "Striking the Right Balance for Transparency–Recommendations to modernize the Access to Information Act," March 2015, online: http://www.oic-ci.gc.ca/telechargements-downloads/userfiles/files/eng/reports-publications/Special-reports/Modernization2015/OIC_14-418_Modernization%20Report.pdf, at pp. 8-9.

It is also consistent with the approach taken in the UK where the Secretary of State has a "further" power to designate public bodies that:

> (a) appear to the Secretary of State to exercise functions of a public nature, or
>
> (b) are providing under a contract made with a public authority any service whose provision is a function of that authority.[10]

In addition, the Organization of American States' Model Freedom of Information Law has also encouraged this approach.[11]

The extent to which FIPPA would apply should be clearly defined and the Act should apply only to the public function that is carried out.[12]

The Act already contains exceptions that respond to the concern that a business or private interest may be harmed by being subject to FIPPA. For example, all public bodies can apply exceptions to access regarding disclosures that are harmful to the financial or economic interests of a public body, disclosures that are harmful to the business interests of a third party, and disclosures that are harmful to personal privacy.[13] These exceptions will protect private interests, including legitimate commercial and economic interests, intellectual property, and privacy.

2.0 RECOMMENDATIONS FOR PART 2 OF FIPPA – FREEDOM OF INFORMATION

2.1 EXCEPTIONS

Section 12 – Cabinet and local public body confidences

The Canadian Union of Public Employees, British Columbia Division, ("CUPE BC") recommends that "the mandatory exemption for the release of information covered by cabinet confidentiality should be ended in favour of a discretionary

[10] Section 5(1), *Freedom of Information Act*, 2000 c. 36, online: http://www.legislation.gov.uk/ukpga/2000/36/contents.
[11] See s. 3, Organization of American States, "Model Inter-American Law on Access to Public Information and its Implementation Guidelines," 2012, online: http://www.oas.org/en/sla/dil/docs/Access_Model_Law_Book_English.pdf.
[12] An example of this can be found in section 6 or Article 19's "Model Freedom of Information Law," 2006, which states that bodies that are carrying out a statutory or public function should be public bodies under the law "provided that the bodies indicated in sub-section (1)(e) are public bodies only to the extent of their statutory or public functions," online: http://www.article19.org/data/files/medialibrary/1796/model-freedom-of-information-law.pdf.
[13] Sections 17, 21, or 22 of FIPPA.

standard."[14] CUPE BC argues the mandatory nature of this exception is excessive and that the government can maintain an appropriate and necessary level of confidentiality using a discretionary exception. CUPE BC also notes that the Cabinet confidences exception is a discretionary exception in Nova Scotia.

The OIPC supports this recommendation with the qualification that only Cabinet, and not the head of a public body, should be able to exercise this discretion. Ministries would be required to withhold information under s. 12(1) when that exception applies but only Cabinet would have the ability to waive the exception when it feels that it is appropriate or beneficial to do so.

A precedent for such a role for Cabinet already exists in s. 16 of the Act, where the head of a public body must not disclose information which could reasonably be expected to harm inter-governmental relations or disclose inter-governmental confidences unless Cabinet consents to the disclosure.

Section 14 – Legal Advice

The Law Society of British Columbia recommends that s. 14 be made mandatory except when the public body is the client and can choose to waive privilege or, where the client is a third party, the client agrees to waive privilege. In all other situations, the Law Society argues, there should be no discretion for a public body to disclose solicitor-client privileged records in its custody or control.

I do not support this recommendation. We are unaware of any situation ever having arisen where this has been an issue under FIPPA. The Law Society has not provided any examples where a public body has disclosed information that was subject to solicitor-client privilege but where the client was not the public body or did not consent to the disclosure.

This is to some extent a situation that is unique to the Law Society, as its oversight over the legal profession makes it the only public body that is likely to have custody of records that are subject to solicitor-client privilege but to which it is not a party. However, we generally do not support amendments to FIPPA that are tailored to the needs of a single public body, particularly in this case, where the public body is able to address the issue itself by exercising its discretion to not provide access.

Section 17 – Disclosure harmful to the financial or economic interests of a public body

The British Columbia Lottery Corporation recommends that commercial Crown corporations should be recognized in FIPPA and should not be subject to the

[14] Canadian Union of Public Employees, British Columbia Division, submission to the Committee, at p. 11.

standard of proof required to demonstrate harm under s. 17. The BCLC says that the s. 17 exception "is not sufficient to allow for protection of certain commercially valuable information and has led to public bodies like BCLC being held to an impossible standard in trying to apply s. 17(1) in some circumstances."

The OIPC does not support a special accommodation for Crown corporations or a lowering of the threshold for applying s. 17.

As public bodies, Crown corporations should be held to the same level of accountability and transparency as public bodies in general under FIPPA. In addition, s. 17 contains an open list of kinds of information that public bodies can refuse to disclose if the disclosure could reasonably be expected to harm their financial or economic interests. The test for applying this exception includes a consideration of the mandate and activities of the public body, including Crown corporations.

Section 20 – Information that will be published or released within 60 days

The Insurance Corporation of British Columbia recommends an addition to s. 20 of the Act where public bodies would not be required to disclose records already provided or available to the applicant. ICBC says that this would encourage more proactive disclosure by public bodies and reduce access to information costs to public bodies (and therefore the public).

The OIPC does not support this recommendation. Such an amendment is unnecessary and would limit the right of access provided by s. 4 of the Act.

OIPC Orders have stated that FIPPA generally does not require public bodies to disclose copies of records that they have already provided to an applicant, either through a previous request or another avenue of access.

However, our Orders have also said that the availability of records through the *Rules of Court* or some other process does not displace or prevent the exercise of a right of access under the Act. Applicants have the right to access records that were unavailable through another process. Applicants also have the right to request access to a record they received through another process if their use of the record is restricted because of the manner in which it was obtained.

Section 22 – Disclosure harmful to personal privacy

When government appeared before the Special Committee on November 18, 2015, they raised concerns about access to information applicants seeking

metadata to "undertake surveillance of the habits of government employees"[15] and said that the Act needs to be modernized to address such issues.

I do not support this recommendation because FIPPA as it is presently worded addresses the issues raised by government.

In fact, my Office recently issued an Order on this very issue, in which an applicant requested metadata from message tracking logs relating to email traffic for several government ministries and public sector entities.

In that case, the OIPC determined that the metadata was personal information and the government must refuse to disclose the requested information under s. 22 of FIPPA. Factors that weighed in favour of the government being able to refuse to disclose the logs included that they could reveal patterns of personal email use or other personal information (such as leave), and that they could reveal personal relationships between employees.[16] Other factors weighed in favour of disclosure, including that the information could subject the government to scrutiny.[17]

While the weighing in this case did not favour disclosure, the adjudicator explicitly recognized that there may be cases that *would* weigh in favour of disclosure, for example, a request for a smaller set of metadata.[18]

Disclosures of metadata should occur where, on balance, it would not be an unreasonable invasion of a third party's personal privacy. A blanket exception that authorized public bodies to withhold metadata would contravene the underlying purpose of the Act.

2.2 SECTION 25 – INFORMATION MUST BE DISCLOSED IF IN THE PUBLIC INTEREST

On November 18, 2015, government suggested to the Special Committee that BC could take a legislative approach to public interest disclosures that is similar to that taken by Newfoundland and Labrador. They said that the Newfoundland and Labrador approach is more measured and privacy-protective.

I do not support this recommendation. There are three reasons I believe that Newfoundland's *Access to Information and Protection of Privacy Act* (ATIPPA),[19]

---

[15] Minutes, Special Committee to Review the *Freedom of Information and Protection of Privacy Act*, Fourth Session, 40th Parliament, Wednesday, November 18, 2015, online: https://www.leg.bc.ca/documents-data/committees-transcripts/20151118am-FIPPAReview-Victoria-n7, at 139.
[16] Order F15-63, 2015 BCIPC 69, at paras. 27 and 28.
[17] At para. 44.
[18] At para. 57.
[19] SNL 2015, c A-1.2.

which is in Appendix 1, contains a weaker and *less* measured public interest disclosure regime than s. 25 of our own FIPPA.

First, s. 25(1)(b) of FIPPA requires a public body to disclose information where disclosure is clearly in the public interest, *whether or not* an access request is made. In contrast, s. 9(1) of ATIPPA only requires a public body to disclose information in the public interest *after* an access request has been made. In other words, ATIPPA's public interest disclosure provision lacks the critical proactive element present in FIPPA's s. 25(1)(b).

The ATIPPA approach would significantly reduce the public's right to information because it relies upon the public knowing what information a public body may possess in order to request its disclosure. This ignores the substantial imbalance of knowledge between a public body and members of the public.

Second, FIPPA's s. 25 (1)(b) provision operates to override any exception to disclosure under the Act. Section 9(2) of ATIPPA only provides that public interest disclosure can override a limited number of provisions in that Act.

My office's recent interpretation of the s. 25 public interest disclosure provision recognizes the privacy interests associated with the access to information exceptions in FIPPA, and discusses how s. 25 can consider those insterests without insulating public bodies from public interest disclosure merely because information falls within a certain class or category.[20]

Third, s. 25(1)(a) of FIPPA sets out only one condition before a public body is required to disclose information to the public, without delay, about matters relating to the environment or to the health or safety of the public or a group of people. The condition is that a risk of significant harm is present in respect of these matters.

Section 9(3) of ATIPPA on the other hand requires that disclosure must not only meet the risk of significant harm test, but that its disclosure must *also* be clearly in the public interest. Requiring both would result in a weaker public interest exception in FIPPA as it would narrow the range of circumstances that would meet the threshold for disclosure.

For these reasons the OIPC does not support amending s. 25 of FIPPA in a manner consistent with Newfoundland and Labrador's ATIPPA.

[20] *Mount Polley Mine Tailings Pond Failure (Re),* 2015 BCIPC 30, at 29, online: https://www.oipc.bc.ca/investigation-reports/1814.

3.0 RECOMMENDATIONS FOR PART 3 OF FIPPA — PROTECTION OF PRIVACY

3.1 ADD BREACH NOTIFICATION TO PART 3 – PROTECTION OF PRIVACY

The Canadian Bar Association supported adding breach notification provisions to FIPPA. The CBA stated that the notification obligations should complement the OIPC's authority to conduct investigations, audits, and inquiries, and that the form of notification should be set out in a schedule to the Act.

I support these recommendations with some qualifications.

A key difference between the OIPC's recommendation for breach notification and that of the CBA concerns a determination from the Commissioner at first instance as to whether an individual should be notified about a breach.

Specifically, the CBA has recommended that the breach notification provisions in FIPPA be modelled on those in Alberta, where the Commissioner is required to make a determination about whether an organization must notify an individual of a breach and must do so on an expedited basis. The relevant provisions in the Alberta legislation state:

> 44.3(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.[21]

Public bodies *should* be required to notify individuals of a breach and that notification should occur "without unreasonable delay" if the breach meets the threshold of when an individual should be notified. My office has recommended that this threshold be "when their personal information is affected by a known or suspected breach, if the breach could reasonably be expected to cause

[21] Section 44.3, *Personal Information Protection Act*, Statutes of Alberta, 2003, Chapter P-6.5.

significant harm to the individual" – but no matter the threshold, the public body should be able to initiate notification to individuals *without a determination from the Commissioner*.

I believe that the Commissioner need not be involved in such a decision at first instance. It will not be necessary in most cases and it could slow notification.

That said, the Commissioner should have an authority to require a public body to notify individuals where a public body has failed to do so. This will be necessary for circumstances when the Commissioner learns of a breach from another party, such as a complainant, and discovers that notification did not occur.

3.2 SECTION 27 – HOW PERSONAL INFORMATION IS TO BE COLLECTED

The Canadian Bar Association recommended that FIPPA be amended to authorize employers to covertly collect information directly from employees without notification in cases where 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. This would permit employers to covertly collect information directly from employees – for example, by using keystroke logging software – for the purposes of managing or terminating an employment relationship.

I do not support this recommendation. Essentially, the CBA is recommending that employers be allowed to disregard the fundamental privacy principle that individuals should have knowledge of how their personal information is collected and the purpose for that collection. FIPPA embodies this principle in its requirement that a public body must notify individuals of the collection of their personal information, and of the purpose for that collection. I can see no reason why this should not also be required in the employment context.

The CBA is concerned that notifying an employee that information is being covertly collected would result in the employee changing their behavior which may frustrate the object of an investigation. However this concern fails to recognize that, while notification must occur prior to the collection of personal information, it does not need to occur at the time of collection. Employers should advise all employees that, during the course of their employment, personal information may be collected covertly during an employer investigation into alleged employee wrongdoing. This prospective notification would satisfy the requirements of FIPPA without compromising any specific investigation.

This covert collection must be limited to those circumstances where it is necessary, such as during ongoing investigations where overt collection could compromise the accuracy or availability of the information. This limitation is

required by s. 26(c) of FIPPA, which states that the collection of information must be limited to that which is necessary for an activity of a public body.

In short, the appropriate means to address the concern raised by the CBA is to prospectively notify all employees that covert collection may occur in certain limited circumstances where it is necessary. It should also be noted that several Orders[22] from my Office have made it clear that covert collection must be used as a last resort, and is only authorized by FIPPA after the employer has attempted to address any workplace concerns openly and directly with the employee, and those attempts have proven ineffective.

3.3 SECTION 30.1 – STORAGE AND ACCESS MUST BE IN CANADA

A number of organizations made submissions to amend s. 30.1. Some of them, largely from or serving the health and education sectors, asked for it to be amended to make it easier for public bodies to store, access, or disclose information outside of Canada, or have asked for authority to disclose where the security standards in another jurisdiction meet those required by FIPPA.[23] Others asked for no amendments to be made, citing privacy issues and the lack of constitutional protections for personal information outside of Canada.

I do not support amending s. 30.1 of FIPPA at this time. The privacy concerns that gave rise to these provisions not only remain unchanged, but have been reinforced by instances of US law enforcement seeking to force cloud providers to disclose information that is stored in data centres held outside of the US.[24] Canadians remain unprotected from unauthorized access and use of their personal information by foreign law enforcement.

What makes this particularly problematic is that the constitutional protections against unlawful search and seizure that we are entitled to in Canada are entirely absent for our personal information that is stored outside of Canada.[25] British Columbians would have little recourse if their personal information was mishandled outside of Canada.

In the private sector, personal information that is stored or accessed outside of Canada is done so with the consent of individuals who provide that information in

---

[22] Order F07-18, [2007] B.C.I.P.C.D. No. 30; Order F15-01, 2016 BCIPC 1.
[23] BCNET, BC School Superintendents Association and BC Association of School Business Officials, Surrey School District #36, the Canadian Bar Association, Insurance Corporation of British Columbia, School District 36, Translink, and the submission from the Health Authorities.
[24] For example, in April 2014, US Magistrate Judge James Francis ruled that Microsoft must provide information stored on its servers in Ireland when there is a valid search warrant from law enforcement, online: https://www.documentcloud.org/documents/1149373-in-re-matter-of-warrant.html. Microsoft is appealing the decision.
[25] This was also discussed in the submission from the BCCLA.

exchange for a product or service. The public sector is different. Most British Columbians do not have any option but to provide their personal information. If a citizen wants health care they must provide personal information to government and to other public bodies. Students in school are required to complete the assignments provided to them. Taxpayers must provide financial information to the Ministry of Finance. These are just some of the many instances where government compels the collection of personal information.

Since individuals are effectively compelled to disclose their personal information, it is appropriate that public bodies are held to a higher standard for the safeguarding of that information. For example, personal information collected by the health sector is some of the most sensitive information held by a public body. Electronic health systems offer significant conveniences and benefits, but also compile and link significant amounts of our personal information. This information has value outside of the health sector, which is why we take its security so seriously. It is appropriate to set a high standard of care for such information.

I acknowledge that these higher standards come at some cost. Yet the extent of these costs should be scrutinized. Several submissions noted the limited options available to public bodies for cloud services hosted within Canada, but recently we have seen the market respond to the demand for storage in Canada. Last year Microsoft and Adobe announced they will be offering cloud-based storage and software applications within Canada and this year Amazon, the largest cloud services provider in the world, made a similar announcement.[26] Developments like these will make it increasingly easier and more affordable for public bodies to access cloud solutions in compliance with FIPPA.

Several submissions indicated that staff and students in the education sector may be unaware of s. 30.1 of FIPPA and how it operates.[27] My office shares that concern. We are working with organizations and school districts to build the capacity in public schools for ensuring that appropriate consent is obtained for the use of cloud-based applications that store or access information from outside of Canada. We have provided workshops on this topic and routinely provide feedback to school districts that are developing consent forms for the use of cloud-based applications in schools. The OIPC has also published guidelines on our website on "Cloud Computing for Public Bodies."

Section 30.1 of FIPPA has been described as requiring "full data-sovereignty" or as "near absolute prohibition" on storage outside of Canada. [28] This hyperbole

---

[26] See Press Release, "Microsoft Cloud Touches Down in Canada," June 2, 2015, online: http://reimagine.microsoft.ca/en-ca/, Spencer Soper and Gerrit De Vynck, "Amazon will open first cloud data storage centres in Canada." January 13, 2016, online: http://www.theglobeandmail.com/report-on-business/international-business/us-business/amazon-will-open-first-cloud-data-storage-centres-in-canada/article28146339/.

[27] See submission to the Committee from School District No. 46 (Sunshine Coast).

[28] See BCNET submission at p. 3, and Canadian Bar Association submission at p. 6.

mischaracterizes s. 30.1. It is not a complete ban and storage or access outside of Canada is authorized for any of the purposes for disclosure listed in s. 33.1 of FIPPA.[29] What's more, in all cases public bodies can obtain the authority to store or access personal information outside of Canada by obtaining consent from the individual whom the personal information is about. In addition, the Minister responsible for the Act has the power to authorize access or storage outside of Canada.[30]

The College of Registered Nurses of British Columbia recommended that the heads of public bodies themselves should be able to authorize storage or access outside of Canada, rather than the Minister responsible for the Act. I do not support this recommendation. That Minister is responsible for considering the overall Act, including balancing the interests of public bodies with the privacy interests of individuals; she or he is not singularly focused on the interests of a single public body and can therefore issue such an order from a more balanced viewpoint.

4.0 RECOMMENDATIONS FOR PART 4 OF FIPPA — THE OFFICE AND POWERS OF INFORMATION AND PRIVACY COMMISSIONER

4.1 SECTION 44(3) – POWERS OF COMMISSIONER IN CONDUCTING INVESTIGATIONS, AUDITS, AND INQUIRIES

The Law Society of BC recommends that s. 44(3) be amended to exclude from disclosure to the Commissioner all records that are subject to solicitor-client privilege. It further recommends that if an issue arises about the validity of a claim of privilege, a new process should be devised that would require the Supreme Court to rule on the issue, rather than the Commissioner, on notice to all persons whose privilege may be affected by an order.

I do not support this recommendation. Section 44(3) is necessary for the Commissioner to carry out her functions under the Act, and appropriate safeguards for confidentiality are already built into the Act. The Law Society's recommendation would create a resource intensive and inefficient duplication of process.

[29] Section 30.1(b), which states that a public body may store or access personal information if "it is stored in or accessed from another jurisdiction for the purpose of disclosure allowed under this Act," should be read with s. 33.1, which lists the circumstances in which public bodies may disclose information inside or outside of Canada.
[30] Section 33.1(3).

Section 44(3) is Necessary to the Commissioner in Carrying out Her Functions

Upon a request for review from an applicant, the Commissioner is responsible for determining whether a public body has correctly applied an exception to disclosure under Part 2 of FIPPA. Those exceptions include s. 14, which allows a public body the discretion to refuse to disclose information in response to an access request where it is protected by solicitor-client privilege.

Public bodies frequently claim s. 14 as authorization to withhold records from applicants. However, it is important to note that of the Orders made in the last five years involving s. 14 issues, that section was determined to be misapplied 21% of the time.[31]

In order for the Commissioner to perform the function of verifying the proper application of this exception, the Legislature conferred express powers and duties to conduct inquiries in private, to require the production of documents for examination and to review the information at issue in strict confidence.

Section 44 confers the Commissioner with the authority to compel the production of records in order to assess whether the exception has been correctly applied. It clearly states that the authority to compel production of records applies despite any other enactment or any privilege of the law of evidence. Further, s. 44(2.1) removes any risk that production of the record has any effect on the privilege:

> 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), the solicitor client privilege of the record is not affected by the disclosure.

This independent oversight additionally acts as a safeguard against any bad faith application of s. 14.

I do not agree with the Law Society's assertion that the Commissioner's jurisdiction to examine privileged documents threatens the protection afforded through solicitor-client privilege.

The Commissioner examines the documents only to determine the validity of the claimed privilege – this is the only way that the Commissioner can determine whether the claimed exemption is valid. The Commissioner does not request the production of privileged records in every instance, but only where it is necessary. The records are not made public or put to any purpose other than verifying that this exemption has been properly applied.

---

[31] Based on Orders made between February 28, 2011 and February 29, 2016, see "Sectional Index," online: https://www.oipc.bc.ca/rulings/sectional-index/.

In addition, if the Commissioner makes an order deciding against an exception for privilege, the Commissioner does not disclose the documents. The Order is directed to the public body claiming privilege; it is subject to an application for judicial review in the Supreme Court of British Columbia, and it would be stayed from the time the judicial review application is filed until the Court orders otherwise. There is no risk of the records being disclosed until all avenues of appeal are exhausted, and then disclosure is made by the public body, not by the Commissioner.

Inefficient Duplication of Process

The process proposed by Law Society would inject an expensive, inefficient, and duplicative adjudicative procedure into the resolution of requests for review under FIPPA, by requiring that records go before the Supreme Court rather than the OIPC to review whether privilege applies. This ignores one of the primary purposes for the creation of administrative tribunals: to relieve the courts of routine adjudications where a tribunal can instead apply its particular expertise to efficiently resolve disputes.

Most requests for review are not limited to single issues; for example, a public body may apply several exceptions to access over a single record, not just solicitor-client privilege. This means that the process suggested by the Law Society would require the duplication of resources, where the OIPC would adjudicate the applicability of certain exceptions to access, but the Supreme Court would adjudicate the applicability of the claim of solicitor-client privilege *over the same record*. This duplication of process has clear negative public policy implications for judicial economy and efficiency in an era where access to scarce judicial resources already results in inadequate access to justice for many parties seeking recourse to the Supreme Court.

In addition, it would necessarily slow the resolution of a complaint to our Office, further delaying an applicant's right to access information.

The Commissioner has had the power to examine and where necessary compel production of records protected by solicitor-client privilege for 10 years in the private sector and over 20 years in the public sector. A considerable body of expertise has been developed during that time and the process, which is efficient and timely, is working well. Through judicial review, the Supreme Court exercises a supervisory function over my Office. The Law Society has offered no evidence to suggest that the present approach does not fully protect solicitor-client privilege, which my Office recognizes is of fundamental importance.

For the reasons set out above, I do not support this recommendation to amend s. 44(3) of FIPPA and believe that an amendment is not necessary.

4.2 SECTION 47(4) – RESTRICTIONS ON DISCLOSURE OF INFORMATION BY THE COMMISSIONER AND STAFF

The submission of the Law Society raises a concern with respect to the protection of solicitor-client privilege that results from s. 47(4) of FIPPA. That section provides that the Commissioner may disclose to the Attorney General information relating to the commission of an offence against an enactment of British Columbia or Canada if the Commissioner considers there is evidence of an offence.

The Law Society maintains that, where the Commissioner is in possession of records to which solicitor-client privilege applies, s. 47(4) leaves open the possibility that the Commissioner could disclose those records to the Attorney General where those records relate to an offense.

I do not support this recommendation of the Law Society. The Law Society is incorrect in its interpretation of s. 47(4) of FIPPA; that section cannot be read to authorize the abrogation of solicitor-client privilege. Its amendment is therefore unnecessary.

This matter has already been addressed by the Supreme Court of Canada[32] and by the Alberta Court of Appeal,[33] which found that this section could not authorize the disclosure of records protected by solicitor-client privilege.

Both Courts found that in order to abrogate solicitor-client privilege, statutory language must be clear, unequivocal, and unambiguous and cannot be taken as authorizing the infringement of solicitor-client privilege by inference or implication.

The Supreme Court of Canada found that the language in s. 20(5) of the federal *Personal Information Protection and Electronic Documents Act* ("PIPEDA"), which is the same as that in s. 47(4) of FIPPA, did not authorize the federal Privacy Commissioner to disclose documents protected by solicitor-client privilege to the Attorney General. This is because that section did not expressly state that it applied despite solicitor-client privilege.[34] Accordingly, the same language in s. 47(4) of FIPPA cannot give the BC Commissioner authority to disclose records to which solicitor-client privilege applies.

For an example of the clear, unequivocal, and unambiguous statutory language that is required to overcome solicitor-client privilege, the Committee could look to s. 44 (3), which applies "[d]espite any other enactment or any privilege of the law

[32] *Canada (Privacy Commissioner) v. Blood Tribe Department of Health*, 2008 SCC 44, at paras. 2, 18, 25-26, and 31.
[33] *University of Calgary v JR*, 2015 ABCA 118, at para. 42.
[34] Blood Tribe, at paras. 24-26.

of evidence" and compare it to s. 47(4) of FIPPA, which does not contain such language.

5.0 RECOMMENDATIONS FOR PART 6 OF FIPPA — GENERAL PROVISIONS

5.1 SECTION 75 – FEES

Automatic Fee Waiver

Some organizations[35] recommend an amendment that would require public bodies to automatically waive fees when a public body fails to meet its legislated timeline for responding to a request.

The OIPC supports this recommendation. My office has monitored the timeliness of government's access to information responses since 2008.[36] There were improvements by 2011 when 93% of access requests received timely responses, but those improvements were lost by 2014 when only 74% of replies met the timelines set out in FIPPA.[37]

This recommendation would offer a statutory-based incentive for public bodies to provide timely responses to access requests.

CONCLUSION

Thank you for giving me the opportunity to express my views on the many recommendations made to this Special Committee. Similar opportunities have been provided to my office by past statutory committees. We are always pleased to assist the Members in your task.

Should you require any further clarification or assistance, I remain available to you during your deliberations.

---

[35] BC Freedom of Information and Privacy Association, the BC Public Interest Advocacy Centre, and the Canadian Centre for Policy Alternatives.

[36] "Special Report - A Step Backwards: Report Card On Government's Access To Information Responses, April 1, 2013 – March 31, 2014," "Special Report - Report Card on the Timeliness of Government's Access to Information Responses, April 1, 2010 – March 31, 2011," "Special Report – Six-month Check up: Review of Government's Timeliness in Responding to Media and Political Parties' Requests, August 6, 2010-February 5, 2011," "Special Report – It's About Time: Report Card on the Timeliness of Government's Access to Information Responses, April 1, 2009-March 31, 2010," "Special Report – Timeliness of Government's Access to Information Responses: Report for Calendar Year 2008."

[37] "Special Report – Report Card on Government's Access to Information Responses, April 2013 – March 2014" at 5.

Summary of OIPC Responses to Recommendations

1. Do not support amending the definition of “contact information” in Schedule 1.

2. Do not support amending the definition of “law enforcement” in Schedule 1.

3. Do not support limiting, to corporations, an amendment that would make the definition of “public body” in schedule 1 consistent with the definition of “local government body and do not support exempting corporations owned for investment purposes.

4. Recommend expanding the criteria that the Minister can consider under s. 76.1 to include entities that perform a public function.

5. Support amending s. 12 which will provide discretion to Cabinet to waive Cabinet confidentiality for the purposes of an access request. The heads of public bodies should not be authorized to exercise the same discretion.

6. Do not support amending s. 14 to make the legal advice exception a mandatory exception.

7. Do not support amending s. 17 to provide Crown corporations with a lower standard of proof to demonstrate harm.

8. Do not support amending s. 20 to authorize a public body to refuse to disclose records that are available elsewhere.

9. Do not support amending s. 22 to authorize public bodies to categorically refuse to disclose metadata on the grounds that it may contain personal information.

10. Do not support amending s. 25 that would narrow the obligation on public bodies to proactively release information in the public interest.

11. Support adding breach notification and associated amendments into FIPPA; do not support a blanket requirement that the Commissioner make a determination about notification to an individual.

12. Do not support amending s. 27 to authorize public bodies to covertly collect personal information directly from employees without notification.

13. Do not support amending s. 30.1.

14. Do not support amending s. 44(3) to exclude, from disclosure to the Commissioner, all records that are subject to solicitor-client privilege.

15. Do not support amending s. 47(4) so that it does not apply to records to which there is a claim of solicitor-client privilege.

16. Support an amendment to s. 75 that would require public bodies to automatically waive fees when a public body fails to meet its legislated timeline for responding to a request.

APPENDIX 1

PUBLIC INTEREST PROVISION FROM THE NEWFOUNDLAND AND LABRADOR *ACCESS TO INFORMATION AND PROTECTION OF PRIVACY ACT*, 2015

Public interest

9.(1) Where the head of a public body may refuse to disclose information to an applicant under a provision listed in subsection (2), that discretionary exception shall not apply where it is clearly demonstrated that the public interest in disclosure of the information outweighs the reason for the exception.

(2) Subsection (1) applies to the following sections:

(a) section 28 (local public body confidences);

(b) section 29 (policy advice or recommendations);

(c) subsection 30 (1) (legal advice);

(d) section 32 (confidential evaluations);

(e) section 34 (disclosure harmful to intergovernmental relations or negotiations);

(f) section 35 (disclosure harmful to the financial or economic interests of a public body);

(g) section 36 (disclosure harmful to conservation); and

(h) section 38 (disclosure harmful to labour relations interests of public body as employer).

(3) Whether or not a request for access is made, the head of a public body shall, without delay, disclose to the public, to an affected group of people or to an applicant, information about a risk of significant harm to the environment or to the health or safety of the public or a group of people, the disclosure of which is clearly in the public interest.

(4) Subsection (3) applies notwithstanding a provision of this Act.

(5) Before disclosing information under subsection (3), the head of a public body shall, where practicable, give notice of disclosure in the form appropriate in the circumstances to a third party to whom the information relates.