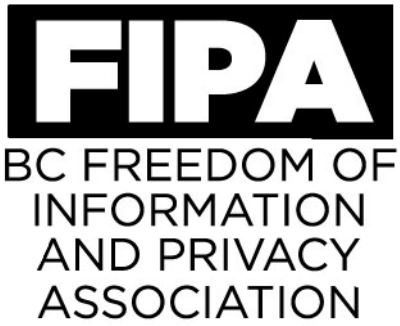

Submission to the Special Committee to Review the *Freedom of Information and Protection of Privacy Act*

October 16, 2015

BC Freedom of Information and Privacy Association
103 – 1093 West Broadway
Vancouver, BC V6H 1E2
T: 604-739-9788 | F: 604-739-9148
fipa@fipa.bc.ca

FIPA would like to acknowledge the Law Foundation of British Columbia. Their ongoing support of our work in the areas of law reform, research and education makes submissions like this possible.

INTRODUCTION

The BC Freedom of Information and Privacy Association (FIPA) is a non-partisan, non-profit society that was established in 1991 to promote and defend freedom of information and privacy rights in Canada. Our goal is to empower citizens by increasing their access to information and their control over their own personal information. We serve a wide variety of individuals and organizations through programs of public education, public assistance, research and law reform.

We thank the Special Committee for the opportunity to provide input for this review of *Freedom of Information and Protection of Privacy Act*. We hope you will find these suggestions helpful.

* * *

When the *Freedom of Information and Protection of Privacy Act* (herein referred to as *FIPPA* or the *Act*) was passed in 1992, it was at the leading edge of freedom of information (FOI) and privacy legislation, and was praised internationally for being the best legislation of its kind.

After almost a quarter century later, it is clear that while the *Act* itself is basically sound, it needs a number of improvements and updates to reflect developments both in government and in technology.

Changes to FOI

On the freedom of information side, the promise of the *Act* was that it would help create a culture of openness within government; that FOI requests would be necessary only as a last resort and that routine release of information would be the rule. Today, however, we frequently see public bodies either failing to create records, or destroying them in order to avoid the possibility of release to FOI requesters. This is a crisis not just for freedom of information, but for the proper conduct of government business.

There have also been victories for transparency since our last submission. The Office of the Information and Privacy Commissioner has taken action to curb the government's practice of redacting large parts of records on the pretext that they are 'outside the scope' of a given request.[1] One ministry estimated that they used this dodge in 25-40 per cent of requests when they could not find an exception that applied.[2] The elimination of this practice will have a huge beneficial effect, primarily for less sophisticated requesters who may be

[1] These orders include Orders F15-23 https://www.oipc.bc.ca/orders/1801 , F15-24 https://www.oipc.bc.ca/orders/1802 and F15-25, https://www.oipc.bc.ca/orders/1803 ,
[2] Order F-15-24, para 16.

unaware of their rights or reluctant to challenge unsupported redactions to the records they receive.

Another victory was the Commissioner's decision to change how section 25 of the *Act*, the public interest override, would be interpreted, in order to better reflect the letter and spirit of the *Act*.[3] We have a great deal to say about this decision, and need for legislative reform to supplement what the Commissioner has done. In fact we are working with the Environmental Law Clinic at the University of Victoria to produce a more detailed proposal, which will be provided to the Committee before the deadline for written submissions in January.

Changes to privacy

On the privacy side, BC has taken a step backward. The 2011 amendments to the *Act* reflect a position—largely criticized by the Committee for being overly intrusive—that the government had advanced during the prior year's statutory review. Other changes to the *Act* suggested that year—such as mandatory breach notification—should have been brought in, but were not.

Further, we will argue that the *FIPPA* be altered to be better-aligned with the *Personal Information Protection Act* (*PIPA*).

This review

We hope this Committee will follow in the footsteps of its predecessor, which had the intestinal fortitude to make recommendations they saw as advancing freedom of information and privacy rights in BC. Regardless of what action the government takes to amend the *Act*, the existence on the record of recommendations by this Special Committee is of great value and importance.

[3] Investigation Report F15-02 https://www.oipc.bc.ca/investigation-reports/1814

HOW GOVERNMENT INFORMATION BECOMES PUBLIC

There are essentially three ways information is released to the public. These are routine release, release through freedom of information and unauthorised informal release.

Routine release

Routine release of information is an absolute necessity for 'open government'. Routine release, also called proactive disclosure, is the forward trend in government information management in all the world's democracies.

FIPPA was amended in 2011 to include a new subsection, 71.1, which gives ministries power to establish categories of records to be routinely disclosed =without a FOI request.

We are currently working with the University of Victoria's Environmental Law Clinic to produce recommendations in this area; we will reserve our input until that report is submitted to you.

Freedom of information requests

The second method of release of information is by request under the *Act*. *FIPPA* provides a complete code for making access requests to government, and a process for the review of decisions to refuse release. The *Act* balances citizens' right to information, and government's need for confidentiality in certain clearly defined, limited circumstances. However, FOI requests should not be—and were not intended to be—the primary method of release.

Unauthorized informal release

The third method of information release is what happens when there is no FOI system, or when the system is dysfunctional. That is unauthorized release, also known as whistleblowing in cases where a public employee "leaks" information. *FIPPA* protects government employees who blow the whistle in good faith in s. 30.3, but there have been repeated calls (including from the Auditor General) for great protection for whistleblowers.

FIPA recommends that the protections provided to whistleblowers be set out in law. This would ideally be done through the creation of a separate law, as was done at the federal level.

PRIMARY AREAS OF CONCERN

In this submission, we are highlighting particular areas of concern rather than attempting to redraft the *Act*. Our comments are based on our experience and the experiences of people who contact our office for assistance. We will also touch on administrative issues which have a large impact on FOI and privacy management.

Regarding freedom of information, the biggest issue is the destruction of records or the failure to create them in the first place. In order for the *Act* to have any relevance, on one side **there must be an obligation to create records,** and on the other side, **records must not be destroyed without proper procedures being followed.**

The issue of **delay** has long been identified as a problem with the *Act* and its administration. **Fees** have also been used to delay or block release under the *Act*, or to discourage requesters.

There is also a need to prevent what we call **'information laundering'**. This involves public bodies hiding behind private contractors or corporations that they fully control, in order to avoid scrutiny.

We will also provide recommendations regarding reform of several exceptions to release in Part 2 of the *Act*. These include exceptions for Cabinet confidences, policy advice, legal privilege and law enforcement.

Finally, the ability to **release information in the public interest** must be clarified. The current interpretation of this section is such that almost no information meets the standard, and we have some alternatives for the Committee to consider.

On the privacy side, we have a number of concerns. The government has an almost unlimited ability to do what it wants with any personal information that it controls. New technology means that **government's ability to data match and data mine** are no longer subject to technical constraints. We need legal protections that are currently missing from *FIPPA* to limit government's uses of personal information, and to prevent data matching and mining.

There is also a serious issue with domestic data storage provisions in s.30.1.Those requirements are being circumvented by the government through the use of tokenization. We are also concerned about the possible effect of the Trans-Pacific Partnership (TPP) Agreement, which appears to undermine this part of *FIPPA* (based on summaries released to date by the federal government).

FREEDOM OF INFORMATION

An obligation to create records and penalties for improper destruction

There can be no public access to records if records are not created. Unfortunately, as noted in several recent reports from the Office of the Information and Privacy Commissioner (OIPC), there has been an increasing trend toward oral government. 4 An "oral culture" is growing in government as officials choose not to record sensitive information or to delete it as soon as possible. This is in complete opposition to *FIPPA*'s legislated purpose of making public bodies more open and accountable.

In September 2012, FIPA filed a complaint with the OIPC about the rapidly increasing number of non-responsive answers to FOI requests.[5] The OIPC's investigation not only confirmed our theory, but also went on to show that the problem is even worse than we originally suspected. Most damning was the finding that the Office of the Premier had seen a dramatic spike in non-responsive FOI requests over the past year. In the 2011/12 fiscal year, 45% of all FOI requests received by the Premier's Office were returned with no responsive records.

Media requesters were hit the hardest by this decline in responsive records. In the 2010/11 fiscal year, Denham's investigators found 37% of media requests filed with the Office of the Premier came back unresponsive. By the end of the 2011/12 fiscal, that number had jumped to 49%. Denham pointed to the growing oral culture as one cause of the problem. Her report showed that most communication in the Premier's Office happens verbally or is classified as "transitory," meaning it is either never written down or quickly deleted.[6]

The Commissioner's report recommended the creation of a legislative "duty to document" to ensure records are in fact created, but the government's response was that it preferred to wait for this Special Committee to consider the questions as part of its review. That time is now at hand.

When government officials avoid scrutiny by failing to create records, this is a threat not only to access, but also to the archival and historical interests of the province. Left without

---

[4] Investigation Report F13-01 Increase in No Responsive Records to General Access to Information Requests: Government of British Columbia https://www.oipc.bc.ca/investigation-reports/1510
See also FIPA's complaint:
https://fipa.bc.ca/new-fipa-calculations-show-dramatic-decline-in-foi-performance-4/

[5] https://fipa.bc.ca/new-fipa-calculations-show-dramatic-decline-in-foi-performance-4/

[6] This is apparently what happened with the investigation of former chief of staff Ken Boessenkool.

records of their predecessors' thoughts, decisions and precedents, other officials are deprived of the benefit of their wisdom – and their folly. History is impoverished and our collective wisdom is diminished. As the saying goes, those who fail to learn the lessons of history are doomed to repeat them; if there is no history, it will be impossible to learn any lessons at all.

FIPA recommends that a positive duty to create and maintain records be incorporated into *FIPPA* or other legislation. This would be a duty to record decision making, and would set out minimum requirements for record keeping in critical areas.

Related to the duty to create records, there should also be a specific duty to retain documents subject to FOI requests or containing personal information, and there should be penalties for intentional destruction or alteration of documents.

Seven provinces and territories, plus the Canadian government have introduced penalties for document tampering into their FOI acts.[7] Canada's *Access to Information Act* includes fines of up to $10,000 and jail terms of up to two years for anyone who tries to deny the right of access to information by destroying, falsifying or concealing records, or counseling another to do so.[8]

Alberta's *Freedom of Information and Protection of Privacy Act* includes fines of up $10,000 for anyone who, among other things, destroys records for the purpose of blocking a freedom of information request.[9]

Earlier this year we were shocked to hear a former of the political staffer of BC's minister of transportation allege that he was ordered to delete dozens of emails relating to the Highway of Tears consultation, which were being requested under the *Act*.[10] The Commissioner is investigating this case, but it is not clear what, if any, penalty those responsible for these deletions could face.

It may be that the current section 74 may be sufficient to deal with cases like this, where destruction of records takes place in the face of a request for information under the *Act*, and appears to be designed to frustrate an actual request being processed by a public servant. Specifically, section 74(1) states that a person who willfully "obstruct[s] the commissioner or another person in the performance of the duties, power or functions of the commissioner or other person under this *Act*" faces a fine of up to $5,000. Section 6 of *FIPPA*, which imposes a duty on public bodies to assist requesters, may also apply.

---

[7] Newfoundland and Labrador, Prince Edward Island, Nova Scotia, Quebec, Manitoba, Alberta and Yukon.
[8] *Access to Information Act*, RSC c. A-1 s.67.1
[9] *Freedom of Information and Protection of Privacy Act*, RSA 2000 c.F.25, s.86.
[10] http://www.huffingtonpost.ca/2015/05/29/former-bc-staffer-alleg_n_7463762.html

It does not appear, however, that current legislation is adequate to deal with situations like this, but where there is not an actual FOI request or OIPC investigation underway. These are cases where records are not kept or where records are destroyed under claims that they are "transitory".

As the Commissioner has noted in her report on FIPA's complaint about no responsive records and in her investigation of the 'quick wins' scandal[11], the move to oral government and failure to keep adequate or any records is a growing problem. She also found "the general practice of staff in that office [the Office of the Premier] is to communicate verbally and in person. We were informed that staff members do not usually use email for substantive communication relating to business matters, and that most emails are 'transitory' in nature and are deleted once a permanent record, such as a calendar entry, is created."[12]

As Commissioner Denham stated regarding the complete absence of records in the investigation of the resignation of the Premier's former Chief of Staff:

> *It appears that government has chosen not to document matters related to the resignation of the former Chief of Staff. The OIPC has investigated hundreds of complaints where government claimed requested records did not exist because they were never created in the first place. There is currently no obligation under* FIPPA *that requires public bodies to document their decision-making. As such, government did not contravene* FIPPA *in opting to conduct a verbal investigation regarding the former Chief of Staff.*[13]

Another major problem is the misunderstanding (either deliberate or through ignorance) of the nature of a transitory record.

Commissioner Denham pointed to another factor in the absence of records – they were being destroyed because they were considered transitory. She expressed doubts that these records would fall under any definition of the word:[14]

> *Staff in the Office of the Premier use the following factors in determining whether a record is transitory:*
>
> - *Temporary usefulness;*
> - *Drafts;*

---

[11] SeeF13-04 Aug 1, 2013 *Sharing of Personal Information as Part of the Draft Multicultural Strategic Outreach Plan* https://www.oipc.bc.ca/investigation-reports/1559

[12] Investigation Report F13-01 p.4

[13] Ibid., p.18

[14] Ibid., p.17

- *Convenience copies of items that originate in other offices or are filed by other departments. Examples: copy of a meeting request, copy of an incoming letter to the Premier;*
- *Only required for a limited time or for preparation for an ongoing record;*
- *Not required to meet statutory obligations or to sustain administrative functions; and*
- *Phone messages.*

Commissioner Denham pointed out that current government policy governing what is to be considered a transitory record was not being followed by the BC government.

> *The Office of the Chief Information Officer ("OCIO"), the central office responsible for information management in government, offers guidance on transitory records on its website, stating that "Transitory records are records of temporary usefulness that are needed only for a limited period of time in order to complete a routine action or prepare an ongoing record." The Ministry of Citizens' Services and Open Government provides a similar definition in its approved government-wide records schedule on transitory records.*
>
> *The OCIO makes it clear that not all drafts or working papers are transitory records. The OCIO also states that some, but not all, email records are transitory. I believe that the determination of whether a record is transitory is not dependent on the medium of communication, but instead depends on whether it is a record of action or decision-making. The Office of the Premier should ensure that its practices regarding transitory records align with the government policy as recommended by the OCIO.*[15]

The Premier's Office is not the only part of government where the word 'transitory' is treated as a magic incantation that allows the destruction of inconvenient or embarrassing records.

In one set of records available on the BC government's open information website, a senior bureaucrat sends an email to staff, telling them to "please delete all drafts of the materials and e-mail correspondence should be treated as transitory."[16] This is not the only case where this has happened.

Records are either transitory or they are not. One does not have the option of "treating them as transitory", and the CIO has set out clear rules and procedures that set out what records are transitory and subject to destruction.

---

[15] Ibid., p.18

[16] http://docs.openinfo.gov.bc.ca/D45786213A_Response_Package_JTI-2013-00073.PDF

BC needs sanctions for the wanton destruction of information, but unfortunately it looks like the government has been moving in the opposite direction. In Bill 5, the *Government Information Act*, the government brought in much-needed measures to improve electronic preservation and access to government records. It updates the Depression-era *Document Disposal Act*, which used to govern how information could be handled, kept or destroyed.

Unfortunately, the good news stops here. Bill 5 failed to bring in a legal duty to document, which is essentially a requirement that bureaucrats create records of what they do. Compounding the problem, Bill 5 also brought in the removal of the possibility of anybody being charged for violating the law regarding the destruction of government records.

Where the *Document Disposal Act* created a provincial offence for violations, Bill 5 abolished that law without preserving that possibility that someone destroying records contrary to the law could face legal consequences.

But this was not the only instance where the BC government absolved wrongdoers of any consequences for their actions.

In Bill 11, which amended the *School Act*, the government brought in some profound changes [17]to how student records are to be handled. Under the previous section 170, it was an offence to "knowingly disclose any information contained in a student record that identifies a student."

Bill 11 still restricts the purposes for which what is now to be called "student personal information" can be used for, but it removes the offence of +improperly disclosing the information.

The common element here is the elimination of either personal or organizational responsibility or liability for the misuse of information held by a public body. Even if these provisions were seldom if ever used, they did serve as a deterrent; that deterrent has now been removed.

Time limits and delay

What started out as a thirty-calendar-day response time has been turned into thirty business days, and the government amended s.10 of the *Act* to give itself a thirty-day extension if they feel "meeting the time limit would unreasonably interfere with the operations of the public body".[18]

[17] http://www.huffingtonpost.ca/2015/03/26/bcs-plans-for-professi_n_6951326.html
[18] FOIPPA s.10(1)(b)

As a practical matter, this delay is at the discretion of the public body, as there is no way for a requester to complain to the Commissioner about the additional time being taken, nor would the matter be heard by that office before the end of the additional thirty-business-day period. This means there is no recourse where a public body takes additional time.

This is a serious problem.

Under s.6, the head of a public body must "…make every reasonable effort to assist applicants and to respond without delay..."

Black's Law Dictionary defines duty as:

> *A human action which is exactly conformable to the laws which require us to obey them. Legal or moral obligation. Obligatory conduct or service. Mandatory obligation to perform.*

A duty is not discretionary, nor subject to whim or budget constraints.

Timeliness is extremely important in the context of FOI. *FIPPA* is perhaps the only statute on the books that is routinely violated without any chance of penalty.

One recent and egregious example can be found in the OIPC mediation summaries.[19] In that case, the public body denied access to audit summaries on the basis of s.12(3). When that failed to convince the OIPC, the public body moved on to s.22. After the privacy argument was shot down, the public body moved on to s.15, saying release could harm investigative techniques, could not point to any likelihood of harm. As a final gambit, the public body resorted to s.21, again shot down because of the weakness of their proposed arguments. After a delay of six months while these increasingly implausible exception claims were raised, the requester finally received the records they were entitled to all along.

This case illustrates the need to have some type of sanction to prevent public bodies from wantonly engaging in this type of high handed and wasteful behavior.

FIPA recommends that a section be added to *FIPPA* that penalizes any person or public body that flagrantly breaches the duty to assist requesters by obstructing access rights or failing to properly document government decisions.

Fees are also used to delay and discourage requests

FIPA has experienced numerous instances where fees have been levied by a public body, only to have them reduced or eliminated on review. We have developed a practice of paying the deposits requested to avoid the delays set out in s.7(4) and s.7(5), but other FOI users

[19] F15-10MS https://www.oipc.bc.ca/mediation-summaries/1817

may not be able to be afford the fees, and either abandon their request or go through an extended delay while they protest the fee.

We have also noticed that some public bodies are refusing to accept requests for fee waivers that accompany the request for information, insisting that such requests can only be made once fees have been assessed and requested. The only conceivable reason for such a demand is s.75(5.1), which requires a head of a public body to respond within twenty days to a request for a fee waiver. **FIPA recommends s.75(5.1) be amended to clarify that a fee waiver can be requested as part of the request for information.**

The first Special Committee agreed that public bodies should be encouraged to complete information requests in a timely manner. They recommended:

> *That public bodies comply with time lines under section 7 of the* Act*, and that in the event of non-compliance with time lines, fees for requests that are not fulfilled within the prescribed time be waived.*

FIPA recommends that an automatic fee waiver for non-compliance be implemented.

The provincial government has had a centralized system for handling of FOI requests for several years, which means that misdirected FOI requests can be sent to the relevant ministry or public body immediately, rather than being transferred from one ministry to another. Section 11 of *FIPPA*, however, still provides a twenty day period for transferring misdirected requests. This is not necessary due to the provincial government's current practices. With that in mind, your immediate predecessors recommended the period be reduced to ten days to prevent misuse and confusion, but this recommendation was not implemented.

FIPA recommends that section 11 of the *Act* be amended to altogether eliminate the twenty day transfer period for public bodies which are part of the new FOI request system.

"Information laundering"

Access to records of 'quasi-governmental' bodies

The trend of the past two decades to outsource work formerly done entirely within government has created new problems for access to records related to public functions.

Some of these responsibilities and functions have been transferred out of the public sector proper and into the sector of organizations that have been called "quasi-governmental" or "quasi-public" bodies. These bodies include multi-governmental partnerships, government-industry consortia, foundations, trade associations, non-profit corporations and advisory groups.

Access to records of subsidiaries of educational public bodies

It will be ten years this year since then- Education Minister Shirley Bond promised to put the subsidiary companies of school boards under *FIPPA*. This promise was made in response to a report about school board subsidiaries losing huge amounts of taxpayer money, which included the recommendation that those subsidiaries be subject to *FIPPA*. This is also an issue for post-secondary institutions in the wake of an unfortunate BC Supreme Court decision in *Simon Fraser University v. British Columbia (Information and Privacy Commissioner)*.[20] That decision was a judicial review of an adjudicator's decision regarding a private company owned and operated by Simon Fraser University (SFU). Some of the relevant facts regarding this company are:

- Its shares are 100% held by SFU
- All its directors are appointed by SFU
- Its physical presence is entirely within SFU without even a distinct office
- All records were held on SFU's campus
- Its activities are 100% dedicated to marketing SFU research

The adjudicator had found that due to these factors, SFU had control of those records for the purposes of *FIPPA* and should therefore provide them to the requester,[21] but Mr. Justice Leask disagreed, finding that "the Delegate erred in law by piercing SFU's corporate veil without applying the proper legal standard for doing so. I also find that the Delegate erred in finding that those records were under the control of SFU and hence subject to the *FIPPA*…"[22]

Justice Leask's decision was appealed, but the BC Court of Appeal shut down its hearing of this case[23] after the death of the requester on the grounds of mootness.

The Commissioner wrote to the Minister of Citizens Services in 2011to express her concern about this situation and to seek amendments to the *Act*.[24] In her letter she pointed out that *FIPPA* provides language that would deal with these subsidiaries, since it covers the subsidiary companies of local government bodies.

It includes in the definition of a "local government body":

---

[20] Simon Fraser University v. British Columbia (Information and Privacy Commissioner 2009 BCSC 1481
[21] Order F08-01 at para 93
[22] Simon Fraser University v. British Columbia (Information and Privacy Commissioner), op cit para 81
[23] BCCA File CA 37692
[24] https://www.oipc.bc.ca/public-comments/1138

(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

By using a similar definition for 'educational bodies', the gap could easily be closed. It would also remove an anomaly in the way education subsidiaries are covered compared to those of municipalities.

The Minister responded that this was a complicated question and would require extensive consultation. That was almost four years ago, and there is no indication that there has been any serious consultation at any point since then.

FIPA recommends that the definition of education body in Schedule A of the *Act* should be amended to mirror the definition of 'local government body'.

Legislative overrides of *FIPPA*

A large number of bills have been passed which take advantage of s.79 to specifically override some or all parts of *FIPPA*. The most recent is Bill 39 currently before the Legislature, the *Provincial Immigration Programs Act*. The Commissioner expressed her concern[25] about yet another use of the legislative override in a situation where the existing protections in the *Act* (in s.22) appear to be entirely adequate to deal with the claimed purpose of the override.

At this point there are 43 laws on the books in this province that include overrides of *FIPPA* in whole or in part. Bill 39 will bring that total to 44, and that is not acceptable, especially since *FIPPA*'s existing exceptions to release appear to be entirely adequate to protect the other societal interests involved.

The problem seems to be based on the preference of public bodies to simply claim the protection of an exception without going to the trouble of showing why it would apply to the records in a given situation. However, exceptions to our information rights should not be made simply for the convenience of the bureaucracy.

FIPA recommends that no further overrides be made to the *FIPPA*, and that existing overrides be examined to see if *FIPPA's* current exceptions would be suitable. Public written justification should be provided for each.

[25] Letter to Minister Bond https://www.oipc.bc.ca/public-comments/1869

Exceptions to release

These exceptions were set out in the original version of the *Act* to balance the right of access to information with various other societal interests.

Over the years a number of these exceptions have come to be more broadly interpreted by government and in some cases by the courts, leading to diminished access rights and ever greater scope for preventing the release of information.

Ideally all exceptions would be harm based. Public bodies should be required to show not just that a particular interest is engaged, but that there is a real risk of harm to that interest if access is given to certain records. The *Act* already contains a number of harms tests, and these have not proven to be insurmountable barriers to protecting legitimate exceptions to release.

Cabinet confidences (s.12)

There was once a time (1968) when conventional legal wisdom was that Crown privilege meant a police officer's notebook could not be released for use in a civil case about a traffic accident.[26]

Since that time, the concept of Crown privilege has been restricted primarily to the deliberations of Cabinet and related records that might reveal what ministers were discussing. The preservation of such confidences is necessary to maintain conventions of responsible government, such as Cabinet solidarity, and to protect the integrity of decision making.

The common law approach to Cabinet confidences in Canada was set out in *Babcock v. Canada*[27] by Chief Justice McLachlin. This involves balancing the public interest in disclosure against the need for Cabinet confidentiality.

> *At one time, the common law viewed Cabinet confidentiality as absolute. However, over time the common law has come to recognize that the public interest in Cabinet confidences must be balanced against the public interest in disclosure, to which it might sometimes be required to yield. Courts began to weigh the need to protect confidentiality in government against the public interest in disclosure, for example, preserving the integrity of the judicial system. It follows that there must be some way of determining that the information for which confidentiality is claimed truly relates to Cabinet deliberations and that it is properly withheld. At common law, the courts*

[26] *Conway v Rimmer* [1968] AC 910; 1 All ER 874 (HL)

[27] Babcock v. Canada (Attorney General), 2002 SCC 57, [2002] 3 S.C.R. 3.

did this, applying a test that balanced the public interest in maintaining confidentiality against the public interest in disclosure.[28]

The rules governing what is not subject to release in response to a request under *FIPPA* are set out in s.12 of the *Act*.

The leading interpretation of this section is found in the 1996 BC Court of Appeal decision in *Aquasource Ltd. v. British Columbia (Information & Privacy Commissioner)*.[29]

That decision turned on wording in s.12(1) as to whether information requested by an applicant must be refused because it "would reveal the substance of deliberations of the Executive Council or any of its committees, including any advice, recommendations, policy considerations or draft legislation or regulations submitted or prepared for submission to the Executive Council or any of its committees."

The Court in *Aquasource* took a very broad view of what was included in "substance of deliberations". In the words of Mr. Justice Donald,

> *I do not accept such a narrow reading of s.12(1). Standing alone, "substance of deliberations" is capable of a range of meanings. However, the phrase becomes clearer when read together with "including any advice, recommendations, policy considerations or draft legislation or regulations submitted ...". That list makes it plain that "substance of deliberations" refers to the body of information which Cabinet considered (or would consider in the case of submissions not yet presented) in making a decision.*[30]

Since *Aquasource* was decided, other provinces with similar or identical provisions in their FOI laws have declined to follow the decision of the BC Court of Appeal, preferring a less restrictive approach which still protects the actual deliberations of Cabinet. One leading case is the Nova Scotia Supreme Court decision in *O'Connor v. Nova Scotia*.[31]

In that case, the court considered two possible interpretations of this section:

> *[20] In this context, the word "substance" may allow two potentially conflicting interpretations. It could broaden the meaning of "deliberations" to include all information upon which the deliberations are based. That was the approach taken by the British Columbia Court of Appeal in Aquasource Ltd. v. B.C. (Information and*

---

[28] Ibid. para 19
[29] Aquasource Ltd. v. British Columbia (Information & Privacy Commissioner) (1998), 8 Admin. L.R. (3d) 236 BCCA
[30] ibid at 39
[31] O'Connor v. Nova Scotia, 2001 NSSC 6

Privacy Commissioner), [1998] B.C.J. No. 1927 when interpreting British Columbia's equivalent provision.

[21] On the other hand, "substance" could refer to Cabinet's actual deliberation process. In other words, only that information touching on the actual deliberations would be protected. This view would significantly limit the s. 13(1) exception in favour of more Government disclosure.

[22] With respect, when comparing the two approaches, I prefer the latter interpretation. To interpret the "substance of deliberations" as protecting all information "form [ing] the basis of Cabinet deliberations", would paint Cabinet confidentiality with too broad a brush. Cabinet may base its deliberations on a variety of data, some of which deserves no protection at all.

FIPA's experience has been that where the s.12 exception is claimed, the government is taking an ever-wider interpretation to the already very broad approach set out in *Aquasource*. Fortunately, the courts do not seem inclined to follow the government's lead, requiring the release of subject headings of agendas for example.

It is imperative that BC's FOI laws reflect the proper protection of the deliberations of Cabinet, and not a notion that any document however vaguely related, falls within this mandatory exception.

Local public bodies

We are at a loss as to why section 12(3), which applies to local public bodies, lacks a parallel to s. 12(2)(c), which applies to Cabinet confidences.

Section 12(2)(c) states that Cabinet confidentiality does not apply to "…information in a record the purpose of which is to present background explanations or analysis to the Executive Council or any of its committees for its consideration in making a decision if

(i) the decision has been made public,

(ii) the decision has been implemented, or

(iii) 5 or more years have passed since the decision was made or considered."

The lack of similar qualifying language in 12(4) allows local public bodies to withhold background materials or analysis in the above conditions not allowed to Cabinet. FIPA finds this to be inappropriate and we recommend that the exception be amended to remedy what we conclude was an unfortunate oversight.

Subsections (5), (6) and (7) provide that records of what are known as Caucus Cabinet Committees are to be treated as actual committees of Cabinet. These subsections were

enacted after the Commissioner found that these committees could not be construed to be actual Cabinet committees for the purposes of s.12.

The Commissioner was correct, and these extensions of what should be an exception limited to the protection of the deliberations of Cabinet are contrary to the spirit (and what was the letter) of the *Act*.

FIPA recommends that:

- **Section 12 should be amended to clarify that "substance of deliberations" only applies to the actual deliberations of Cabinet or a local public body.**
- **Section 12 should be made discretionary and that the time limit for withholding records should be reduced to 10 years.**
- **Section 12(4) should have similar qualifying language to s. 12(2) (c)**
- **Section 12(5)(6) and (7) should be removed.**

Advice and recommendations (s.13)

The purpose of the exception in s.13 is to allow for the unfettered discussion and development of policy within government by public servants for decision by their political masters.

As the BC government itself once stated:

> *The Ministry submits that the underlying intent of section 13 is "to allow full and frank discussion of advice or recommendations within the public service, preventing the harm that would occur if the deliberative process of government decision and policy making was subject to excessive scrutiny." (Submission of the Ministry, paragraph 5.02) (emphasis added)*
>
> *A common step in the deliberative process of government decision making is the preparation of a discussion paper which lists and evaluates recommendations developed by the Public Body for change in policy or programs. This process requires full and frank discussion within the Public Body of the advice and recommendations which are developed. This is exactly the type of information which section 13 is intended to protect from disclosure. (Reply Submission of the Ministry, paragraph 5)* (emphasis added)[32]

[32] Order 215-98. See also Order No. 193-1997 p7

Clearly the intent of the legislature in the design of s.13 was to protect the legitimate interest of society in allowing public servants to freely and candidly provide advice or recommendations to decision makers in government without fear of premature disclosure.

However, the legislature only intended to protect the advice and recommendations of public servants, not to create a blanket that could be thrown over any information provided for use in the deliberative process.

In a speech to the 2007 BC Information Summit, former Attorney General Colin Gabelmann (the Minister responsible for the original *FIPPA*) pointed out that the intention of the legislature in drafting s.13 was very different from what the BCCA in *College of Physicians* thought it was:[33]

> *Section 13 was so clear and obvious that there was not a word spoken by any member of the House on it during the committee stage debate. Not a word! Somehow, the B.C. Court of Appeal in 2002 determined that the Information and Protection of Privacy Commissioner got it wrong in interpreting the words "advice and recommendations" in this manner. They said the trial judge was wrong, too, in concurring with the commissioner.*
>
> *I have to tell you that the Appeal Court quite simply failed to understand our intention - the intention of the legislature - when using these words as we did…. I can't think of another example where the Appeal Court got something as wrong as they did here. The Act should not really have to be amended because it is really clear in every way, but unfortunately an amendment has been our only option for the past five years. A government which believes in freedom of information would have introduced amendments in the first session of the legislature after that Appeal Court decision to restore the act's intention.*
>
> *Now, the Appeal Court decision means that the secrecy advocates in government are using the two sections of the Act in tandem to refuse to allow public access to material that is at the very heart of the principles of freedom of information. This is an outrage and must be remedied.*

The legislature also foresaw the potential for abuse in subsection (1) if there was an overbroad reading of the words advice and recommendations. In subsection (2) they added an extensive list of types of information which could not be withheld under the rubric of 'advice and recommendations', even though they may have formed much of the basis for the advice or recommendation.

---

[33] See: http://thetyee.ca/Views/2007/10/15/FOI/

The John Doe decision

Earlier this year, the Supreme Court of Canada had the opportunity to pronounce on the nature of the policy advice exception in a case called *John Doe v. Minister of Finance*.[34]

In that case, the high court held that a series of drafts were covered under s.13 of the Ontario law (which also covers policy advice) and did not have to be released to the requester.

In the words of the court,

> *Protection from disclosure would indeed be illusory if only a communicated document was protected and not prior drafts. It would also be illusory if drafts were only protected where there is evidence that they led to a final, communicated version. In order to achieve the purpose of the exemption, to provide for the full, free and frank participation of public servants or consultants in the deliberative process, the applicability of s. 13(1) must be ascertainable as of the time the public servant or consultant prepares the advice or recommendations. At that point, there will not have been communication. Accordingly, evidence of actual communication cannot be a requirement for the invocation of s. 13(1). Further, it is implicit in the job of policy development, whether by a public servant or any other person employed in the service of an institution or a consultant retained by the institution, that there is an intention to communicate any resulting advice or recommendations that may be produced. Accordingly, evidence of an intention to communicate is not required for s. 13(1) to apply as that intention is inherent to the job or retainer*.[35]

There is a great deal of concern that information which was previously available to requesters through FOI will now be denied by public bodies, forcing another lengthy legal fight to determine just how far this exception can be stretched.

And it appears to stretch quite far indeed.

In a decision following the *John Doe* decision, the BC Court of Appeal upheld the decision of a judge of the BC Supreme Court in a case involving a request not for audits, but the summaries of audits that had been released without an FOI by other health authorities.[36]

The Commissioner has also identified audits as the types of records that should be released as best practices for open government.[37]

---

[34]John Doe v. Ontario (Finance) 2014 SCC 36 http://scc-csc.lexum.com/scc-csc/scc-csc/en/item/13633/index.do

[35] Ibid., para 51

[36] Provincial Health Services Authority v. British Columbia (Information and Privacy Commissioner), 2013 BCSC 2322

It would be perverse if the Supreme Court of Canada's ruling in *John Doe* becomes the means by which public bodies are able to prevent the release of information through the FOI process – especially when that information is the type that the Commissioner would recommend to be released proactively.

We ask that you eliminate the uncertainty, and take action to amend s.13 to restore it to its proper role: of protecting the advice of public servants to their political masters.

FIPA recommends that the s.13 advice and recommendation exception be amended to include only information which recommends a decision or course of action by a public body, minister or government.

Legal privilege (s.14)

The operation of this section has come to our attention as a barrier to transparency.

In 2010 the OIPC handed down a ruling in a case involving the Vancouver School Board (VSB).[38] The VSB claimed that a review of its policies and practices prepared by a lawyer was exempted from release because it was covered by s.14. The Adjudicator disagreed, pointing out that there was no indication in the retainer letter or elsewhere that the lawyer was retained for the purpose of providing the public body with legal advice.[39]

Subsequent orders have shown that where public bodies retain lawyers to provide reports which do not themselves constitute or contain legal advice, they are now careful to include a line in their retainer that the lawyer is also retained for the purpose of providing legal advice.[40]

This loophole allows public bodies to avoid releasing reports (especially controversial ones) by retaining a lawyer through an agreement that mentions legal advice, and then employing s.14.

Clarifying this section to prevent this practice would not undercut the importance of the legal privilege exception, but would properly frame its application in the FOI context. This is not a problem exclusive to BC: The Ontario Commissioner is now hearing a case involving a university whose hockey team was involved in sexual assault allegations. The university hired a law firm, and the firm then engaged a consultant to conduct an investigation of the incident. A journalist requesting the report was told that it was privileged because the law

---

[37] Investigation Report F11-02 Investigation Into The Simultaneous Disclosure Practice Of BC Ferries https://www.oipc.bc.ca/investigation-reports/1243 Appendix A

[38] Order F10-18

[39] Ibid., at para 34.

[40] See for e.g. Order F12-05 (2012 BCIPC No. 6), para 23: https://www.oipc.bc.ca/orders/923

firm had hired the consultant. The hearing has taken place and we are awaiting the Commissioner's decision. If this maneuver is successful in blocking access to the consultant's report, we can expect to see this type of activity take place in this province unless the law is changed.

Law enforcement (s.15)

A recent decision by the Information and Privacy Commissioner has brought up the question of when an investigation is open for the purpose of the *Act*.

In a response to FIPA's complaint about the mysterious RCMP investigation into the Ministry of Health data breach firings, Information and Privacy Commissioner Elizabeth Denham found that it was "not unreasonable" for the BC government to believe an RCMP file was not really closed, because it would be reopened "if and when" the government's own related investigation was completed.[41]

Responding to a FOI request from FIPA, the BC government claimed an RCMP investigation could be harmed by releasing the requested records. The RCMP sent an email supporting the government's position, but after the hearing, and before the OIPC made their decision, the RCMP closed the file and told the BC government that it would be reopened "if and when" the latter completed their investigation into the matter.[42]

This leaves some uncertainty about when an investigation can be finally defined as concluded, and it also raises the question of whether

FIPA recommends that s.15(1)(a) be amended to add the word "active" before "law enforcement matter".

Release in the public interest (s.25)

There has been important and positive change in the way this section is being interpreted by the Commissioner since the last review of the *Act*.

In a major report released in July of this year[43], Commissioner Denham made a major reinterpretation of the law dealing with release of information in the public interest without a freedom of information request.

---

[41] https://fipa.bc.ca/wordpress/wp-content/uploads/2015/09/OIPC-resp-ltd-re.-Cowan-letter-F15-61767.pdf

[42] See: http://www.vancouversun.com/health/RCMP+probe+fired+health+workers+never+happened/11106928/story.html

[43] Investigation Report F15-02 https://www.oipc.bc.ca/investigation-reports/1814

Commissioner Denham has told the government to have all other departments to look through their files for information that must be released under a new interpretation of Section 25 of *FIPPA*.

Section 25(1) of *FIPPA* requires a public body to release information "without delay" without a FOI request where there is "…a risk of significant harm to the environment or to the health or safety of the public or a group of people", or that is "for any other reason, clearly in the public interest."

According to the Commissioner's new interpretation, the element of urgency implied by the words "without delay" applies to the release of information by the public body. In other words, all information that is clearly in the public interest must be released without delay – not just emergency information.

This new interpretation is similar to one we have suggested to this Committee's predecessors, and which was included as a recommendation in the 2010 Special Committee Report.[44]

In our view, and that of the Commissioner, the current interpretation of section 25, which claims it contains an 'implied' temporal requirement is in error. Information need not be of an urgent nature to be disclosed in the public interest. The only temporal requirement set out in law is that of the public body to disclose, without delay, information about a risk of significant harm to the environment or to the health or safety of the public or a group of people, or which is otherwise clearly in the public interest.

The Commissioner had previously released another investigation report on the lack of use of s.25 by public bodies in 2013, stating that the reading-in of a temporal requirement into s.25(1)(b) has resulted in a situation where; "[t]he intention of Legislature with respect to this provision is not being achieved."[45]

In that report, the Commissioner had also recommended the BC government amend the law to remove the 'urgency' requirement.[46]

FIPA's preferred solution to this problem would be for s.25 to be amended to restore its original intent. The purpose of the provision is to ensure that, regardless of other interests that may tend to influence the decision of a public body, the final decision regarding the disclosure of records is made in the public interest.

FIPA recommends that s.25 be amended in accordance with the Commissioner's recommendation to remove the temporal requirement.

---

[44] Op cit, Recommendation 19

[45] Investigation Report F13-05 – Information & Privacy Commissioner for B.C., p. 36

FIPA will supply this Special Committee with a more detailed submission on possible implementation strategies for the new approach being put forward by the Commissioner (and hopefully supported by amendment of the *Act*).

[46] Ibid.

PRIVACY PROTECTION

The BC government has had a record of accomplishment in the privacy sector. It has shown leadership among the provinces, first by introducing the *Personal Information Protection Act* and second by strengthening the privacy provisions of *FIPPA* to counter the potential impact of foreign legislation when the personal information of British Columbians is disclosed to foreign-owned corporations.

However, there are some storm clouds on their way.

During the 2010 consultation, the provincial government made a number of requests for greater ability to share personal information in the name of "citizen-centred services". Your predecessors in 2010 were not convinced and specifically rejected many of the government's recommendations.[47] However, the government went ahead and instituted those changes in 2011.

Domestic data storage (s.30.1)

This section was added to the *Act* in 2004 after a huge controversy over the outsourcing of pharmacare information to a subsidiary of the American company Maximus.

The amendment followed the recommendations in an extensive Special Report by the Office of the Information and Privacy Commissioner entitled *Privacy and the USA Patriot Act – Implications for British Columbia Public Sector Outsourcing*.[48] That report recommended that *FIPPA* be amended to, among other things,

> *Prohibit personal information in the custody or under the control of a public body from being temporarily or permanently sent outside Canada for management, storage or safekeeping and from being accessed outside Canada;*[49]

This provision has ensured that all public bodies in BC store personal information in this country, but it is now under threat.

The first and most serious threat was just revealed last week when the federal government unveiled the Trans-Pacific Partnership agreement.

---

[47] Report of the Special Committee to review *FIPPA* 2010, p.22 "We do not support the idea of indirect collection of personal information, without consent, except for the extenuating circumstances specified in the existing Act, nor the addition of an implicit consent clause. With regard to the recommendations promoting information sharing, we do not think a compelling case was made in general terms to expand the consistent-purpose provision, and the language of the amendments was not specific enough to guide committee members during their deliberations."

[48] OIPC Oct 29, 2004 https://www.oipc.bc.ca/special-reports/1271

[49] Ibid., Recommendation 1 (a)

Buried in one of the various backgrounders were two bullet points about the effect of the TPP on Electronic Commerce. They read as follows:

- *Prevents governments in TPP countries from requiring the use of local servers for data storage.*
- *Prevents governments in TPP countries from demanding access to an enterprise's software source code.*[50]

The TPP clearly is designed to prevent governments from having laws on their books which require domestic data storage, and s.30.1 of FIPPA will clearly contravene the TPP if it was to be ratified.[51]

In case there was any doubt about what the drafters of the treaty intended in this chapter, the federal government provided a cheerful example of how it would work to help businesses:

> ***Bringing down virtual barriers***
>
> *An entrepreneur has developed a proprietary system for electronic payments that protects both the consumer and vendor with every transaction. When he heard about the TPP, he knew it would help him expand his business into important Asian markets. He is pleased with the TPP's dedicated Electronic Commerce Chapter, which will help establish an environment that is more conducive to the type of work he and his customers do.* ***Of particular interest to this entrepreneur are provisions that enable the free flow of data across borders and prevent the Parties from requiring the local establishment of computing facilities.*** *That means that not only can he sell his technology to online vendors in TPP markets right from his home in Canada, but there will be more demand for his technology as online vendors in TPP markets expand their own business to take advantage of the benefits of the TPP.*[52] (emphasis added)

It is possible that these provisions may not apply to *FIPPA*, but this would require that the *Act* be covered by what is known as a 'reservation'. A reservation is usually contained in an appendix to the treaty in question and it lists existing laws of the various signatories which are specifically exempted from the operation of the treaty's general provisions.

---

[50] http://www.international.gc.ca/trade-agreements-accords-commerciaux/agr-acc/tpp-ptp/understanding-comprendre/13-E-Comm.aspx?lang=eng

[51] It should be noted that the Canada-Europe Trade Agreement (CETA) does not use this language. http://www.international.gc.ca/trade-agreements-accords-commerciaux/agr-acc/ceta-aecg/text-texte/18.aspx?lang=eng

[52] Ibid.

If no reservation has been made for *FIPPA*, two possible outcomes flow from that fact.

The first is that BC amends the law to remove the prohibition on public bodies storing or making personal information accessible outside Canada. This would significantly reduce the protection for our personal information and would open up data storage for public bodies to companies and organizations from outside the country, possibly making out information subject to their laws, including the *USA PATRIOT Act*.

The second possibility is that BC does not amend *FIPPA*'s data protection sections, thereby opening up the federal government to lawsuits under the TPP from companies prevented from bidding on (and making a profit on) storage of public sector controlled personal information. It is unclear exactly how much that could cost the federal government, but other cases have seen settlements in the millions of dollars.[53]

FIPA has used freedom of information requests to try to find out how the BC government has been discussing the TPP and *FIPPA*, so far without success. The first request—which asked about a conference call between the Ministry of Citizens' Services and the Office of the US Trade Representative (USTR)—resulted in no responsive records, despite the fact we had already obtained information about the call from the USTR through the American FOIA system.[54] The second, which asked for Ministry of International Trade's records relating to the TPP's potential effects on *FIPPA*, has been delayed until November.

We are perturbed by this at least partly because during the 2010 review of *FIPPA*, the government submission requested that the domestic data storage requirements be scrapped. Your predecessors rejected this proposal out of hand:

> *…we are not prepared to recommend amending the provision in the* Act *prohibiting the storage of information outside Canada to take into account changes in information technology. We believe it is important to protect the integrity of records held by BC public bodies as much as we can.*[55]

We urge this Special Committee to call whatever government officials necessary to get to the bottom of this situation. This is especially important, as the federal government has now stated it will not provide the promised text of the TPP agreement until sometime after the federal election.[56]

---

[53] Bowater

[54] https://fipa.bc.ca/us-trade-representative-calls-bc-privacy-law-a-trade-barrier/

[55] Special Committee report 2010, op.cit, p.22

[56] http://www.cbc.ca/news/politics/canada-election-2015-tpp-text-release-delay-1.3270806

There is no firm timetable for when the final text of the TPP will be released. In fact, we are still waiting for a final text[57] of the Canada Europe Trade Agreement (CETA) which the federal government announced with much fanfare in October 2013.

Tokenization and BC government contract with Salesforce.com

There is another aspect to the domestic data storage provisions of the *Act*, one that is playing out behind closed doors in government. If the Special Committee is inviting government officials to testify, we would suggest you also ask them about a contract signed in October 2013 with CRM software giant Salesforce.com, based in San Francisco.

This contract is referred to in a memo from the CIO to Assistant Deputy Ministers and ministerial information officers urging them to contract the office of the CIO for more information on how to use the services offered by Salesforce.com, despite it being a US-based company.[58]

The government is of the view that tokenization of the personal information is a means to avoid the domestic data storage provisions of *FIPPA*.

Commissioner Denham had been contacted by the BC government about the possibility of using tokenization to get around the domestic data storage requirements in s.30.1 of the *Act*. The Commissioner released her response in June 2014.[59]

This is how Commissioner Denham described tokenization:

> *Tokenization involves replacing information in an electronic record with a randomly-generated token. The original information can only be linked to the token by what is known as a 'crosswalk table'. Tokenization is distinct from encryption; while encryption may be deciphered given sufficient computer analysis, tokens cannot be decoded without access to the crosswalk table.[60]*

In her response to the CIO, the Commissioner stated that the government's plan could be in compliance with *FIPPA* if tokenization of the information being stored outside Canada was "adequate" and the personal information was not identifiable without the 'crosswalk table' which had to be stored in Canada and not be accessible outside Canada. In this situation, the Commissioner states that the information would no longer be 'personal information' for the purposes of the *Act*, so there would be no prohibition on storing it outside the country.

---

[57] A consolidated text is available here. http://www.international.gc.ca/trade-agreements-accords-commerciaux/agr-acc/ceta-aecg/text-texte/toc-tdm.aspx?lang=eng

[58] http://docs.openinfo.gov.bc.ca/d11384614a_response_package_ctz-2014-00009.pdf

[59] Ibid.

This leaves us with a number of questions.

Is the government's tokenization adequate? We have no idea to what extent information is being tokenized before it is being sent to Salesforce. The Commissioner states in her letter that she has concerns about the level of tokenization and the possibility of the individuals being identifiable from the untokenized information. If only the names of individuals—and not the rest of their personal information—are being tokenized, then clearly that would be inadequate. We need to know what is happening with this personal information that is being sent to the United States.

It is difficult if not impossible to supervise the level of tokenization across the government and in each individual case. What might be adequate tokenization for a person living in a large city may not be adequate for someone living in a small town.

FIPA recommends that the BC government and other public bodies be required to make public the details of any tokenization system they use to avoid the operation of the domestic data storage requirements of *FIPPA*.

Posting of personal information contained in government reports

The reports in question deal with the mysterious Ministry of Health data breach firings (the McNeil report) and with excessive executive payments at Kwantlen University (the Mingay Report). Both reflect unfavourably on the government and senior officials.

In order to avoid posting the reports, the government had claimed that *FIPPA*'s section 33.2 prevented them from posting the reports—which contained personal information, and might run counter to the "reputational interests" of public servants or public figures—online, where they would be "accessible" outside Canada.

Strangely, other public bodies like the BC Lottery Corporation go out of their way to post the personal information of lottery winners on their website, but the BC government has not seen fit to require them to put a stop to this practice.

In response to our complaint[61], the OIPC has now confirmed and clarified that *FIPPA* would not be an impediment to the posting of such reports online – it just requires the minister to make an order.[62]

---

[60] OIPC public comment June 16, 2014 Updated guidance on the storage of information outside of Canada by public bodies https://www.oipc.bc.ca/public-comments/1649

[61] https://fipa.bc.ca/wordpress/wp-content/uploads/2015/01/Complaint-Letter-re-BC-govt-refusal-to-post-vg1.pdf

[62] https://fipa.bc.ca/wordpress/wp-content/uploads/2015/08/OIPC-letter-to-FIPA-re-s33-150730.pdf

Clearly this is not the best way to ensure that these reports are posted, and in the letter to FIPA the OIPC stated that the law should be changed to eliminate this anomalous two-step procedure:

> *This matter can, and the Commissioner believes should, be put to the Special Committee reviewing* FIPPA*, which was struck in May 2015, so that the Legislature can assess whether and how to authorize the online publication of personal information contained in such reports. This would be consistent with the broad purposes of* FIPPA *and in particular the need to hold government accountable in s. 2. Our Office encourages stakeholders to bring any matters of concern of this nature to the attention of the Special Committee.*[63]

FIPA recommends that the *Act* be amended to allow posting of government reports and similar publications without the need for a ministerial order.

When privacy rights collide with government programs

Government bodies routinely collect, use and disclose a huge amount of sensitive personal information about citizens. Often this information is collected under the force of law in situations where receiving a license, benefit or a government service depends on the individual providing the information.

Consider the range and detailed nature of the personal information gathered by public bodies in the course of administering, for example, health care services, income assistance programs, family and child support services, and education. It is clear that government possesses an intimate and detailed picture of all our lives.

This information is used every day to make life-affecting administrative decisions about individuals – decisions that affect our family lives, our jobs, our financial and physical well-being, and even our freedom.

The collection of much of this information is necessary for government to carry out its programs properly and efficiently. But the possession by government of a vast amount of information about our personal lives can also present a serious threat to such constitutionally-guaranteed rights as privacy, freedom of expression and freedom of assembly.

Most people would agree that citizens in a democracy should know as much as possible about their government. But how much should a government know about its citizens? That is to say "what about privacy?" After all, if government can look into your health, your mental state, your consumer habits, your finances, even your sexual behavior, and it can go

[63] ibid

further and share this information across ministries and assemble it into comprehensive files on each citizen, what privacy is left to protect?

Governments have been well aware of this dilemma for some time, and this awareness is reflected in privacy protections that have been created in the *Canadian Charter of Rights and Freedoms* and in privacy legislation at both the federal and provincial levels.

The Supreme Court has much to say about our constitutional right to privacy. As stated *R. v. Dyment*,

> *Grounded in man's physical and moral autonomy, privacy is essential for the well-being of the individual. For this reason alone, it is worthy of constitutional protection, but it also has profound significance for the public order. The restraints imposed on government to pry into the lives of the citizen go to the essence of a democratic state.*[64]

The right to privacy with respect to documents and records was addressed by the Supreme Court in *R.* v. *Plant* as follows:

> *In fostering the underlying values of dignity, integrity and autonomy, it is fitting that s. 8 of the* Charter *seek to protect a biographical core of personal information which individuals in a free and democratic society would wish to maintain and control from dissemination to the state. This would include information which tends to reveal intimate details of the lifestyle and personal choices of the individual.65*

The basic question this committee faces is where the balance should be struck between privacy rights and government demands for increased powers to match and mine data.

Collection, use and disclosure of personal information by private-sector agencies of government operating under contract as social service providers

We have raised this previously with your colleagues reviewing the *Personal Information Protection Act* (*PIPA*), which governs the private sector in this province.

There are several hundred BC public bodies, most of which engage private sector entities to assist with some provision of services, at least some of the time. In such cases, these agencies may have access to highly sensitive personal information of citizens. Such information is collected by the private sector entity, on behalf of or for the public body, in order that the citizen may obtain needed public services, including health care, mental health care, social services or education services, among other things.

---

[64] *R. v. Dyment* [1988] 2 S.C.R. 417

[65] *R.* v. *Plant*,[1993] 3 S.C.R. 281, para. 19

Typically, the public body is obliged to take the position that the private sector agency is a "service provider" under *FIPPA*, and to require the agency to execute an agreement in respect of the protection of personal information. The agreement typically contains terms by which the service provider agrees to comply with the duties under the *Act* in respect of all the information collected by it for the purposes of the services. The public body may also require employees or contractors to sign confidentiality agreements, and other related agreements such as security terms.

But this is not always the case. Sometimes the public body and the private sector agency do not adequately identify the obligations and laws that apply; sometimes the parties fail to execute the necessary agreements. The impact of these failures is that often each of the parties implicitly relies on the other to protect the information and neither does an adequate job.

This becomes particularly problematic when information is collected by an agency for social services purposes, and then disclosed by that agency into a government information system. Who is responsible for the data collection? Who is responsible for notifying the individual of their rights, responding to access requests, protecting the data during the collection and disclosure process? Is consent necessary for the collection of the personal information, or not? When the individual is dealing with a private sector service provider but the services are funded in whole or in part by government, what does the individual know about their privacy and confidentiality?

These are important questions because in order for the individual to trust the agency enough to provide reliable information, he or she needs to understand his or her rights. The problem is, their rights under *FIPPA* and *PIPA* are quite different.

PIPA requires the individual to provide some form of consent for the organization to collect, use and disclose her personal information. This consent must be voluntary, and informed. This regime is fundamentally different than that under the *FIPPA* which is not consent-based and permits collection, use and disclosure where relates directly to or is necessary for an operating program or activity of the public body, or for a wide range of other permitted purposes. Further, *FIPPA* permits personal information to be disclosed by the public body to another public body for a very long list of purposes. The reality is that once a public body collects an individual's personal information, it can be shared with other public bodies under *FIPPA* much more readily than it could be by any organizations subject to *PIPA*.

While there are good reasons that *FIPPA* is not consent-based, it is unquestionably a less rigorous standard. Currently, there are several government systems now operating or in development which will require personal information being transferred by agencies subject to *PIPA*, to public bodies subject to *FIPPA*.

The effect of this move towards further integration of systems and social services agencies with public bodies is to apply the less rigorous standard of *FIPPA* to private sector organizations. What this means is that the individual client seeking assistance and believing the services to be provided on a confidential basis may not be aware that their personal information is being disclosed, as a matter of course, to a public body that may then decide—quite lawfully, under *FIPPA*—to further share the personal information with other public bodies.

Take, for example, a single parent, coping with poverty, struggling to adequately provide for his or her children, while dealing with their own emotional or physical health problems. Increasingly we are seeing small non-profits collaborating to share space and resources. Their funding and services might be funded in whole or in part by different public bodies; one may be funded by the Ministry of Social Development and Social Innovation, another by the local health authority, the third by the Ministry of Children and Family Development.

That parent might have come through the doors seeking help from one agency, and end in using all of them. This may be an efficient way to ensure the individual can get all the support available, but if the agencies share their information amongst themselves on their own behalf and then disclose that information to the public body funding some or all of their services, the individual must be provided notice and an opportunity to consent or not. Suddenly the parent seeking confidential assistance for a mental health concern may find that her personal information has been shared among the agencies, and by each of them with their funder. Now this parent may fear that the agency is reporting her to the government and may withdraw. Ultimately the client's trust is undermined and the agency's ability to provide services is compromised.

This is not just a theoretical concern. We conducted a study several years ago, and looked at a number of agencies in BC. We found that for clients who access several services provided by different programs and potentially linked to funding from several Ministries, the failure to maintain confidences could have far-reaching implications. Our stakeholder survey suggested that failure to maintain client confidences could severely affect access and referrals to many community social services.[66]

Our research indicates that clients will refuse to access the services they need if their confidentiality is not assured. When that happens, social services costs, health costs and costs to society inevitably increase. The data is less reliable because people are less trusting, and less truthful. There are poorer outcomes for families and wasted taxpayers dollars on systems that are ineffective. Thus the value of the government's investment in such electronic systems is diminished as is the reliability of the data collected.

Clearly, it is essential that individuals understand where their personal information goes. Even though the *FIPPA* does not require consent for a public body to collect personal information, *PIPA* does require consent. Agencies that are subject to *PIPA* but provide service under service-provider contracts with public bodies must be made aware of their obligation to provide notice to individuals (as they are required to do as the agent of the public body) *and to obtain the individual's consent*, as they are required to do as an organization subject to *PIPA*.

This may not require an amendment. It is possible that the problem can be remedied through a policy change that would add a clause to the standard Privacy Protection Schedule required by the Ministry of Technology, Innovation and Citizens Services.

We recommend the Committee amend *FIPPA* to provide that where an organization collects personal information on behalf of a public body, it is obliged to ensure that the individual is provided notice and that all the rights including the right to refuse consent and be advised of the consequence of such refusal, apply in the circumstances.

Mandatory breach notification

At present there is no requirement for notification of the Commissioner if a public body suffers a privacy breach.

The Commissioner pointed out in her report on Health Authority Privacy Breach Management[67] that breach notification is required by a directive in the federal public sector and is legislatively mandated in Newfoundland and Nunavut, while six jurisdictions require breach notification in their health information statutes.

Your colleagues on the Special Committee that reviewed *PIPA* earlier this year recommended mandatory breach notification and reporting for the private sector in BC.

FIPA recommends that there should be mandatory breach notification for public bodies included in *FIPPA*.

* * *

[66] Survey done for Culture of Care or Culture of Surveillance 2010 https://fipa.bc.ca/wordpress/wp-content/uploads/2014/03/Culture_of_Care_or_Culture_of_Surveillance_March_2010.pdf

[67] Special Report Examination of British Columbia Health Authority Privacy Breach Management Sept 30, 2015

CONCLUSION

This Committee's predecessors reviewed this *Act* in 2010 and made a number of valuable recommendations to improve information and privacy rights in this province.

Equally important is the fact that they rejected a number of proposals from the government which would have undermined those rights.

We urge you to consider carefully the recommendations we have brought before you, and thank you for the opportunity to have presented them.