Submissions on Review of the Freedom of Information and Protection of Privacy Act

Submission to
The Special Committee to Review the Freedom of Information and Protection of Privacy Act
February 2010

[With subsequent minor corrections]

BC Freedom of Information and Privacy Association
103 - 1093 West Broadway, Vancouver, BC V6H 1E2
Ph: 604-739-9788 • Fax: 604-739-9148
Email: info@fipa.bc.ca • Web: www.fipa.bc.ca

FIPA wishes to acknowledge the Law Foundation of British Columbia
for their ongoing support of FIPA's activities in the areas of law reform,
research and public education

BC Freedom of Information and Privacy Association
103 - 1093 West Broadway, Vancouver, BC V6H 1E2
Ph: 604-739-9788 • Fax: 604-739-9148
Email: info@fipa.bc.ca • Web: www.fipa.bc.ca

Introduction

The BC Freedom of Information and Privacy Association (FIPA) is a non-profit society established in 1991 for the purpose of advancing freedom of information, open and accountable government, and privacy rights in Canada. We serve a wide variety of individuals and organizations through programs of public education, legal aid, research, public interest advocacy and law reform.

* * *

When the *Freedom of Information and Protection of Privacy Act* was passed in 1992, it was at the leading edge of FOI and privacy legislation, and actually received praise internationally as the best legislation of its kind.

Eighteen years later, as members of the organization that started the movement to get the act passed, and was involved in its writing, we can say with some authority that the act has not fared well over the years and that B.C. has fallen behind other jurisdictions in providing open government, transparency and privacy protection to its citizens.

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 only be necessary as a last resort and that routine release of information would be the rule. That fees would not be a barrier to access, and that the heads of public bodies would make every reasonable effort to assist applicants and respond without delay to each applicant openly, accurately and completely.

The reality of freedom of information in this province has turned out quite differently, as almost any FOI requester who appears before you will be happy – or unhappy – to tell you.

This committee is composed of both Liberal and NDP members, and one of the facts you need to hear is that freedom of information has suffered under both NDP and Liberal governments. The effort to eviscerate the FOI act and make it progressively more difficult to use began seriously under the NDP administration in 1998. These efforts were greatly increased and became much more sophisticated under the Liberal administrations of the last decade. Just lately, we have started receiving reports that the situation has grown even more difficult for those sturdy citizens who dare to make FOI requests and are still standing.

Privacy protection has fared somewhat better in the province. The current administration introduced a very good *Personal Information Protection Act* covering the private sector in 2003 and made some positive amendments to the privacy part of the Freedom of Information and Protection of Privacy Act in 2004. But all is not well on the privacy front: a government project that is

currently moving forward in BC called the "Social Sector Integrated Case Management Project" poses a greater threat to the privacy of BC citizens than any in modern memory.

FIPA made submissions to the two previous Special Committees examining this Act, and we are pleased to have the opportunity to do the same in 2010. We hope you will find our suggestions and observations helpful.

A number of our recommendations will be the same as last time, and several were accepted by your predecessors. New recommendations will deal with problems that have emerged over the last six years.

The problems our previous recommendations were designed to remedy have worsened over time, as you will see. The six years between committee reports have seen some of them develop into what can only be described as a crisis. If action is not taken soon, irreparable damage may be done to the information and privacy rights of British Columbians.

We dare to hope that this committee will rise to the challenge of restoring and advancing freedom of information and privacy rights in this province. These rights need champions within government, and at this moment in time, we look to you.

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

If 'Open Government' is the goal, 'routine release of information' is what gives it reality. Routine release, or proactive disclosure, is the trend in government information management in all the world's democracies, and it has been embraced by organizations as large as the government of the United States,[1] the City of Vancouver[2] and the City of Nanaimo.

Because most if not all records now exist in electronic form, much more government information should be available on government websites.

Under the Obama administration's Open Government Initiative, government agencies must preserve and maintain their electronic information, publish it online in "open formats" and proactively release it using modern technologies instead of waiting for Freedom of Information Act requests

The City of Vancouver has created a major project to put increasing amounts of data up for the public on what it calls its Open Data website.

If this kind of proactive release can be accomplished by governments both larger and smaller than the government of BC, there is no reason why this province should not also be taking steps down this road.

In fact, your predecessor committee made two important recommendations regarding routine disclosure and taking advantage of technological developments.

> *Recommendation No. 2 – Add a new section 2(3) stating that the Act recognizes that new information technology can play an important role in achieving the purposes outlined in subsection (1) [of the FOIPP Act], particularly with respect to promoting a culture of openness and informal access to information and by enhancing privacy protection.*
>
> *Recommendation No. 5 — Add a new section at the beginning of Part 2 of the Act requiring public bodies — at least at the provincial government level — to adopt schemes approved by the Commissioner for the routine disclosure of electronic records, and to have them operational within a reasonable period of time.*

[1] http://fipa.bc.ca/home/news/230
[2] http://data.vancouver.ca/

FIPA recommends that a new s.2(3) be added to require the use of information technology to advance the purposes of the Act, particularly the routine release of information.

We urge you to highlight the need for this move to greater openness in your recommendations. This information was paid for with taxpayers money, we own it and we should have access to it.

Freedom of Information Requests

The second method of release of information is by request under this Act. FOIPPA provides a complete code for making access requests to government and a process for the review of decisions to refuse release. This is a vital link in the chain of citizens' ability to find out what their governments are doing, and provides a balance between the rights of citizens to information and legitimate requirements for confidentiality in certain clearly defined, limited circumstances. However, it should not be and was not intended to be the primary method of release.[3]

Unauthorized informal release

The third method of information release is what happens when there is no FOI system, or the system is dysfunctional. That is unauthorized release, also known as whistleblowing if it is unauthorized or a 'leak' if it is done by a public body. FOIPPA protects government employees who blow the whistle in good faith in s. 30.3.

We will not be discussing whistleblowing in this submission, but **FIPA recommends that the protections provided to whistleblowers should be set out in law, probably in a separate law as exists at the federal level.**

[3] See exchange between Premier Campbell and MLA Joy MacPhail, Hansard May 18, 2004 – "Hon. G. Campbell: As I mentioned, I don't have that information. The member can certainly ask through the FOI for all that information to be gathered."

Primary areas of concern

We have not undertaken a redrafting of the Act. Our objective here is to highlight areas of particular concern with the act and its interpretation, 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 how well management of FOI and privacy functions.

Regarding freedom of information, there are two sides to a single existential coin. 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, most recently by the Commissioner and by FIPA in studies done in 2009. **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 fully controlled by public bodies to avoid scrutiny of how they spend public funds for public purposes. A recent BC Supreme Court decision has made this problem into an emergency.

BC is far more accommodating to government secrecy than other provinces because of its courts' interpretation of what constitutes information that would reveal **cabinet confidences.** Government has been working consistently to expand this interpretation.

The use of the exception for **advice and recommendations** under s.13 of the Act has become ever more prevalent and must be brought back within the scope the legislature originally intended.

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 this committee to consider.

On the privacy side, we have a number of concerns. The government's almost unlimited ability to do what it wants with personal information within its control has to be restrained. 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 FOIPPA to keep this from happening.

There is now a **gap between the protections enjoyed under the *Personal Information Protection Act* and FOIPPA**, and that gap must be closed. In particular,the definitions of "consistent use" "collection" and disclosure" are too broad. In particular, section 34 should be amended to provide that the purpose of a use or disclosure of personal information is a consistent purpose only if a person might reasonably have expected such a use or disclosure.

Freedom of Information

1. An obligation to create records and penalties for improper destruction.

There can be no public access to records if records are not created. Unfortunately, it has been widely noted that 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 the FOIPP Act's legislated purpose of making public bodies more open and accountable.

The "oral culture" phenomenon first gained some notoriety in BC in 2003 when a senior public official publicly admitted "I don't put stuff on paper that I would have 15 years ago…Civil servants are choosing not to write things down, or at least I am." Regarding email, he stated "I delete the stuff all the time as fast as I can."[4]

The fallout was that the official was forced to "clarify" his statements and re-affirm the application of the FOIPP Act to all government records. But there is no question that the informal practices that he revealed continue.

In order to avoid unwanted scrutiny, many public servants communicate more with phone calls, avoid making notes, fail to keep minutes of meetings, and use e-mail which they delete in contravention of the *Document Disposal Act*.

More recently we have seen thousands of e mail records subject to a court order for production disappear, be destroyed, then miraculously reappear.

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 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 "dumbed down". 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.

The best solution to this problem would be to create a "culture of openness" within government to replace the oral culture. This was declared to be one of the purposes of the FOIPP Act when it was passed, but the deeply set culture of secrecy within governments in our adversarial democracies does not die easily.

FIPA recommends that a positive duty to create and maintain records be incorporated into the FOIPP Act or other legislation – a duty to record decision-making, and minimum requirements for record keeping in critical areas.

[4] Ken Dobell, quoted in *The Province*, October 2, 2003, Michael Smyth's column.

There should also be a specific duty to retain documents subject to FOI requests or containing personal information, and there should be penalties for malicious destruction or alteration of documents.

Seven provinces and territories, plus the Canadian government have introduced penalties for document tampering into their FOI acts.[5] 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.[6]

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.[7]

FIPA recommends that a section be incorporated into the FOIPP Act to penalize any person or public body that deliberately destroys documents against the authority of the FOIPP Act and the *Document Disposal Act*.

2. Time limits and delay

As noted in our introduction, we support the previous Special Committees' recommendation to have s.2(3) of the Act clearly state that routine release of information is expected to be the primary method of public access.

We have appended a copy of our 2009 study *FAILING FOI: How the BC Government flouts the Freedom of Information Act and stonewalls FOI requests*. The study looked at FOI requests for general (non-personal) records, which are often made in order to scrutinize government policies and actions and hold the government accountable. The government usually considers there is more at stake politically with these requests and in the past has marked them for special handling.

FIPA found that, over the three-year period from 2006 to 2008, the rate at which the government violated statutory timelines for general requests was 51.5%. And if the 30-day extension of time a ministry can "award" to itself in extraordinary circumstances were removed, *almost 60% of general requests would have taken more than the 30 day period originally intended by the act as the norm for responding.*

This is a very serious problem.

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

---

[5] Newfoundland and Labrador, Prince Edward Island, Nova Scotia, Quebec, Manitoba, Alberta and Yukon.
[6] Access to Information Act, RSC c. A-1 s.67.1 [check cite]
[7] Freedom of Information and Protection of Privacy Act, RSA 2000 c.F.- 25, s.86.

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.

This means a duty is not discretionary, or subject to whim or budget constraints. The pattern of delay indicates clearly that this duty is not being taken seriously, and the time has come to implement penalties for a head who fails to carry out their statutory duty.

As the Alberta Court of Appeal stated in a privacy decision released last week,

> The PIPA process exists to serve the larger public interest in a number of ways, as well as vindicating privacy rights both generally and specifically. The time rules intend to promote inquiry efficiency and the expeditious resolution of privacy claims. Timeliness is a necessary feature of how PIPA serves the public interest**.** Academic debates about privacy encroachments years after the fact are not likely what the Legislature had in mind. Both claimants and respondents have a reasonable expectation of timely resolution of complaints.[8]

Timeliness is just as important in the context of FOI. FOIPPA is perhaps the only statute on the books that is routinely violated without any chance of a penalty being imposed on those who violate it.

What is clear is that the statutory duty to assist is not being met, and that there are no negative consequences for the head of a public body who does not carry out this duty.

FIPA recommends that FOIPPA be amended to provide for penalties for heads of public bodies who flagrantly breach the duty to assist.

Reasons for Delay

One reason for the delay is that amendments made in 2002 redefined what a 'day' is under the FOIPPA, moving from 'calendar' to 'business' day and giving the government more time to respond. **This anomaly should be removed and a day should mean a calendar day, not a business day.**

Another problem is that under s.10(1) public bodies can give themselves another 30 days to complete requests if they feel "meeting the time limit would unreasonably interfere with the operations of the public body".[9] There is no scrutiny of how this is done, and it is not practical to ask the Commissioner to review such decisions. The granting of time extensions should not be solely within the hands of public bodies.

---

[8] *Alberta Teachers' Association v. Alberta (Information and Privacy Commissioner)*, 2010 ABCA 26

[9] FOIPPA s.10(1)(b)

Which brings us to the role of the Commissioner's office in providing additional time extensions beyond the 30-day extension public bodies may grant themselves. According to the OIPC, requests for additional time extensions under s. 10 have been granted at an 80 plus percent clip since 2006.[10] That could be because the requests are well founded, or because the OIPC is generous with time extensions or a combination of both. What is not in question is that, as a practical matter, when these extensions are granted there is no way to appeal that will not result in significant additional delays.

Another problem is that section 20(3) allows public bodies to get 60 days free by promising to release the records publicly within 60 days. However, if they decide not to release the documents, then the FOI request is reset at day one. The wording of this section amounts to an encouragement to act in bad faith for a public body seeking to delay release.

FIPA recommends that s.20(3) be amended to provide for immediate release of all requested records to the requester if the records in question are not made public after the 60 day period.

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). Other users may not be able to be afford the fees and abandon their request, or go through an extended delay while they fight the fee battle with the public body.

We have also heard disturbing stories about public bodies 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 20 days to a request for a fee waiver. To our view, there is no reason why this obligation could not be met by a letter of response saying that a request for a waiver would be looked at while assessing whether or not to charge a fee.

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:

> ***Recommendation #3: 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.***

[10] Response to inquiry by FIPA, September 2009

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

As you have heard from provincial government officials, a new centralized system for handling of FOI requests has been created which is stated to be more efficient. Requests will be sent to the relevant ministry or public body immediately, rather than being transferred among ministries. If that is the case, it appears that the 20 day period now provided in section 11 for transfer of requests to another public body would not be required in the provincial government.

FIPA recommends that section 11 of the Act should be amended to eliminate the 20 day transfer period for public bodies which are part of the new FOI request system.

Delays at the Office of the Information and Privacy Commissioner

According to the Commissioner's annual report, the goal is to have more than 50 percent of requests for review completed within the statutory 90 day time limit. [11]

This is a sad commentary on how long it can take to have a request for information dealt with. However, we do not see how this problem can be remedied by a change to the Act. More resources will be required, resources which will be hard to come by in difficult economic times.

However if the government adds unfunded responsibilities or make cuts to the OIPC budget, this would obviously make this problem worse, and we urge you to recommend stable funding for this important office.

3. "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.

Any reduction in the Act's coverage of institutions that are funded by taxpayers, carry out public policy as determined by Legislatures, or deliver

[11] 2008-2009 Annual Report, Office of the Information and Privacy Commissioner for British Columbia, pp. 9-10.

public services on behalf of government, is a reduction of transparency, accountability and democracy. It also costs taxpayers money by allowing more opportunity for malfeasance.

The clearest example of this phenomenon is the removal of BC Ferries from the scope of the FOIPP Act in 2002. In 2009, information came out through federal securities regulatory filings that the executives and directors of BC Ferries were being paid amounts far in excess of what comparable public sector executives and directors were receiving. Would these huge amounts have been paid if BC Ferries were subject to FOI requests? We think not.

FIPA recommends that the FOIPP Act be extended to all public and quasi-public bodies and to records created by or in the custody or control of alternate service providers.

Access to records of service providers

The second Special Committee stated, "The Committee is persuaded that there needs to be some explicit assurance in the Act that alternate service delivery does not affect access rights, particularly as recent amendments have established that privacy rights are protected [under these arrangements]". They made this recommendation:

> ***Recommendation No. 4 – Amend section 3 to clarify that records, including personal information, created by or in the custody of a service provider under contract to a public body are under the control of the public body for which the contractor is providing services.***

This recommendation has become even more important in light of the BC Supreme Court decision in *Simon Fraser University v. British Columbia (Information and Privacy Commissioner*.[12]

That decision was a judicial review of an adjudicator's decision regarding a private company owned and operated by Simon Fraser University. 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

[12] *Simon Fraser University v. British Columbia (Information and Privacy Commissioner* 2009 BCSC 1481

The adjudicator found that because of these factors, SFU had control of those records for the purposes of FOIPPA and should therefore provide them to the requester.[13]

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*…"[14]

FIPA believes this is too narrow an approach and we will be intervening in the BC Court of Appeal hearing of this case[15]. While it may be suitable for tax cases or search and seizure, it completely ignores the need for the public to have access to records relating to how public funds are spent by public bodies. And the potential consequences would be disastrous for FOI and accountability for public funds.

If it is not overturned by the BC Court of Appeal, this decision means every public body in the province will be able to avoid FOI requests by creating wholly owned or controlled subsidiary corporations to act as repositories of records. If that is allowed to happen, the effectiveness and purpose of this law will be severely impaired and the public accountability it provides will be lost.

SFU and its associated companies made the argument that if the records in question were released, then it would impair their businesses or business relationships with SFU and others.

If this is the real concern, then *FOIPPA*, under its business harm exemption at section 21, provides a test for addressing those concerns. Those concerns might be perfectly valid, but public bodies should have to provide the evidence to meet the test of harm and confidentiality set out in section 21 or other exceptions which may apply.

Another argument relied upon heavily by SFU was the contrast between the definitions in the *FOIPPA* of "local government body", which includes corporations created by the local government or their directors, and the definition of the "public body" which does not. This, they say, suggests that the intent of the Legislature was that the legislation would not cover subsidiary corporations of public bodies which are not municipalities.

In our view it was not necessary for the Legislature to say "or wholly owned and controlled subsidiaries" in relation to every public body, because the "custody or control" test provides the appropriate outcome as well as a functional and substantive approach.

---

[13] Order F08-01 at para 93

[14] *Simon Fraser University v. British Columbia (Information and Privacy Commissioner)*, op cit para 81

[15] BCCA File CA 37692

However, given the importance of the issue, it may be time for the Legislature to amend the Act to specifically include all companies incorporated by public bodies, not just those incorporated by municipalities and their directors. This change would have the benefit of removing all uncertainty, and ensuring that public funds spent by a public body for a public purpose would be subject to scrutiny under FOIPPA.

The alternative is to wait, and hope that the BC Court of Appeal agrees with FIPA and the Commissioner that "custody and control" is sufficient to ensure that the records of these subsidiary companies can be requested under FOIPPA.

If the BC Court of Appeal agrees with Mr. Justice Leask, and this subsidiary arrangement succeeds in avoiding the *FOIPPA*, it will give virtually every public body carte blanche to set up its own information laundering subsidiary, eviscerating the purpose and effect of the *FOIPPA.*

Maintain section 21, harm to third-party business interests

In a related matter, it will doubtless be suggested that section 21(1)(b) be amended to remove the word 'supplied'.

This type of amendment was recommended by some parties, including the government in its corporate submission during the last review of the Act. Fortunately, both the Special Committee and the Information and Privacy Commissioner agreed that the balance in the FOIPP Act between access to information and protection of third party business interests is the right one, and is consistent with other Canadian access laws.[16]

FIPA recommends that the existing wording and interpretation of s.21 be maintained.

4. 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.[17]

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.

[16] See 2004 Special Committee report p. 23 and Information and Privacy Commissioner submission p. 21
[17] *Conway v Rimmer* [1968] AC 910; 1 All ER 874 (HL)

The common law approach to cabinet confidences in Canada was set out in *Babcock v. Canada*[18] 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 did this, applying a test that balanced the public interest in maintaining confidentiality against the public interest in disclosure.[19]

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

The interpretation of this section is governed by the 1996 BC Court of Appeal decision in *Aquasource Ltd. v. British Columbia (Information & Privacy Commissioner).*[20]

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.[21]

---

[18] *Babcock v. Canada (Attorney General)*, 2002 SCC 57, [2002] 3 S.C.R. 3.
[19] Ibid. para 19
[20] *Aquasource Ltd. v. British Columbia (Information & Privacy Commissioner)* (1998), 8 Admin. L.R. (3d) 236 BCCA
[21] ibid at 39

Other provinces refused to follow BC approach

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*.[22]

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 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*. There are a number of hearings and Judicial Reviews now underway where the government is seeking to widen the scope of *Aquasource*. Each of these cases carries the risk that what is already an unduly broad interpretation of this exception will be expanded even further.

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.

---

[22] *O'Connor v. Nova Scotia*, 2001 NSSC 6

Section 12(2)(c) states that Cabinet confidentiality does not apply to "…[I]nformation 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 conditions not allowed to Cabinet. FIPA finds this to be completely inappropriate and we recommend that the exception be amended to remedy what we conclude was an unfortunate oversight.

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)

5. Advice and Recommendations (s.13)

The need to amend s.13 was urgent in 2004 when the previous Special Committee recommended it.[23] The situation has deteriorated even further since that time, and can now be legitimately be called a crisis.

What has been happening to the s.13 exception bears a number of similarities to what has been happening under s.12:

- A court decision extended the scope of the exception well beyond what the legislature intended and previous interpretation.[24]
- Other provinces have taken a less restrictive approach.[25]
- The government has used the broad exception to prevent the release of information.
- The government has sought to expand the exception even further.

[23] *Enhancing the Province's Public Sector Access and Privacy Law*, Recommendations 11 and 12.
[24] College of Physicians of British Columbia v. British Columbia (Information and Privacy Commissioner), [2002] B.C.J. No. 2779 (C.A.)
[25] See Appendix 1 for a description of the analysis most commonly used by various jurisdictions across this country, and in British Columbia until 2002.

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 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)[26]

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.

The legislature also clearly 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.

The 'Dr. Doe' Decision

In *College of Physicians of British Columbia v. British Columbia (Information and Privacy Commissioner)* or 'Dr. Doe' as it is more commonly known, the Court of Appeal based its decision primarily upon a lengthy examination of solicitor-client privilege, ending in application of the s.14 exemption to the documents in question. Almost as an afterthought, the Court also said that the documents would also be exempt from disclosure under s.13. The Court applied an extremely broad interpretation of the meaning of the words advice and recommendations. The court focused on the rule of statutory

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

interpretation that where the legislature uses two different words, they must be given two different meanings in order to avoid the creation of a tautology.

The decision has been widely criticized in this province, and its interpretation of 'advice and recommendations' rejected by the courts in other provinces.

In his letter to the Minister of Labour on April 25, 2007, the Information Commissioner provided an illuminating précis of the shortcomings in the BCCA's analysis and obsession with the avoidance of tautology.

> One example of the courts treating the words "advice" and "recommendations" interchangeably is *Thomson* v. *Canada (Deputy Minister of Agriculture)* (1992), 89 D.L.R. (4th) 218 (S.C.C.). In *College of Physicians and Surgeons*, the Court of Appeal cited *Thomson* on another point, but did not mention that the Supreme Court of Canada in that case treated the word "recommendation" as meaning "advice". At pp. 242-243, Cory J., for the majority, said that "'[r]ecommendations' ordinarily means the offering of advice". Further, there is ample authority for the proposition that legislation may sometimes contain words that have the same or overlapping meanings. See R. Sullivan, *Driedger on the Construction of Statutes*, 4th ed. (Toronto: Butterworth's, 2002), at p. 173. See, also, *R.* v. *Goulis* (1981), 33 O.R. (2d) 55, at p. 61 (Ont. C.A.). Drafters with knowledge of the legislature's objective will use apparent repetition in a statute's wording to avoid potential misunderstanding or problems with its administration (or, where applicable, to preserve parallelism between two language versions). Where there is reason to believe words are deliberately included in the legislation, any presumption against tautology––mentioned by the Court of Appeal in *College of Physicians and Surgeons*, is rebutted. See R. Sullivan, *Driedger on the Construction of Statutes*, at p.162"

In a speech to the 2007 BC Information Summit, former Attorney General Colin Gablemann (the Minister responsible for the original FOIPPA) 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:[27]

> 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.

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

> 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.

Other Jurisdictions

Although this decision has been the law in this province since 2002, other jurisdictions have rejected the approach taken by the BCCA.

In 2005, the Ontario Court of Appeal rejected this approach in *Ontario (Ministry of Northern Development and Mines) v. Ontario (Assistant Information and Privacy Commissioner)* [28].

In that case, the Ontario government put heavy emphasis on the BCCA decision in *College of Physicians of British Columbia v. British Columbia (Information and Privacy Commissioner*. The Ontario Commissioner, supported on judicial review by a Superior Court judge, used the traditional interpretation of advice and recommendations (similar to the one used by the BC Commissioner up to the BCCA decision in 2002). The Ontario Court of Appeal agreed this interpretation of "advice or recommendations" was reasonable and said this:

> "The most fundamental principle of interpretation is that words must be understood in light of the context and purpose of the whole statute.
>
> The purposes of the statute is stated by s. 1 of the Act [Ontario's *Freedom of Information and Protection of Privacy Act*] to be
>
> 1. The purposes of this Act are,
>
> (a) to provide a right of access to information under the control of institutions in accordance with the principles that,

[28] Op cit note 13 *Ontario (Ministry of Northern Development and Mines) v. Ontario (Assistant Information and Privacy Commissioner)*, [2004] O.J. No. 163 (Div. Ct.), aff'd [2005] O.J. No. 4048 (C.A.), leave to appeal refused [2005] S.C.C.A. No. 564]

(i) information should be available to the public,
(ii) necessary exemptions from the right of access should be limited and specific, and
(iii) decisions on the disclosure of government information should be reviewed independently of government; and

(b) to protect the privacy of individuals with respect to personal information about themselves held by institutions and to provide individuals with a right of access to that information.

In my view, the meaning of "advice" urged by the Ministry would not be consonant with this statement of purpose. The public's right to information would be severely diminished because much communication within government institutions would fall within the broad meaning of "advice", and s. 13(1) would not be a limited and specific exemption. I conclude, in the words of the Divisional Court that "the Commissioner's interpretation complies with the legislative text, promotes the legislative purpose, and is reasonable."(para 27-8)

Expansion of the scope of Dr. Doe

The government has been constantly trying to expand the scope of the s.13 exception, with the most outrageous example dealing with submissions to the government consultation process following the last Special Committee's examination of this Act.

FIPA took part in a consultation with 26 other groups, but also filed a FOI request for all the submissions to this process. the Ministry disclosed the "amendment possibilities" and complete copies of a number of "stakeholder submissions". The Ministry disclosed some but not all the "stakeholder submissions", claiming that they constituted "advice and recommendations provided by stakeholders to the Ministry" in 2006 during one of a series of consultations with stakeholders.

These were responses to a consultation process. Other government ministries, such as the Ministry of Attorney General, carry out web-based public consultations on government initiatives, including draft legislation. The public's comments, similar in nature to the information in dispute here, are posted on government websites for all to see with no suggestion that s. 13 (or the federal equivalent) applies to them. The Ministry of Attorney General's web-based consultation papers also contain a warning that freedom of information legislation may require the Ministry to disclose the public's responses to consultations.

The Commissioner's Adjudicator noted "there is some irony in the Ministry's use of FIPPA to withhold stakeholders' comments on potential amendments to FIPPA itself".[29] Despite finding the Ministry had not properly exercised its discretion to release the submissions, she still found that under the Dr. Doe

[29] Order F09-02 para 31

criteria these qualified as 'advice or recommendations' and were subject to the s.13 exception.

FIPA does not agree with this interpretation, and we are currently seeking judicial review of this decision.[30] We are hopeful that the court will find this situation not just ironic, but also wrongly decided. However if this decision stands, submissions to consultations will become 'advice', and another large swath of what should be public records will be locked away from scrutiny.

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. The situation was dire when your predecessors looked at FOIPPA, and it is more so now. As you will see from the "Dr. Doe" report appended to this submission, we have actually set out how such an amendment could be made (new portions underlined).

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.

6. Release in the public interest (s.25)

This section puts a duty on the heads of public bodies to immediately release information in circumstances where release is in the public interest.

Successive interpretations of this section have resulted in a standard which is unreasonably high ("urgent and compelling") and which is not found anywhere in the language of the section. It was added by interpretation by the Commissioners[31] and by judicial review.

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 taken in the public interest.

It is unfortunate that section 25 of the FOIPP Act has not fulfilled its purpose for a variety of political and bureaucratic reasons. Chief among these is the subjectivity of the term "public interest" and the question of who has the privilege of defining it.

A recent Supreme Court of Canada decision which discusses the nature of the public interest and how a court should determine whether or not it applies in the context of defamation litigation casts doubt on the approach taken in this province.

---

[30] *BC Freedom of Information and Privacy Association v. Office of the Information and Privacy Commisioner* Vancouver Registry S-097178

[31] Order F02-38

In *Grant v Torstar Corp*.[32], the court enunciated a new defence to defamation claims of "responsible communication on matters of public interest". The Court found that reporting on issues in the public interest engaged the guarantees of freedom of expression set out in the Charter of Rights and Freedoms.

Supreme Court set out principles for lower courts to determine whether a matter was on a matter of public interest.

> Public interest may be a function of the prominence of the person referred to in the communication, but mere curiosity or prurient interest is not enough. Some segment of the public must have a genuine stake in knowing about the matter published.[33]

The Court also made clear that judges should not be overly restrictive in their determination of what is (or is not) in the public interest.

> The public has a genuine stake in knowing about many matters, ranging from science and the arts to the environment, religion, and morality. The democratic interest in such wide-ranging public debate must be reflected in the jurisprudence.[34]

The Supreme Court has explicitly laid down new ground rules on what constitutes the public interest, in light of Charter values and their importance to society. It is vital that the past interpretations of public interest must be reassessed in light of the Supreme Court's decision in *Grant*. That reinterpretation should not be left to individual requesters seeking redress from the Commissioner or the courts. It should be done by the legislature, and this committee should recommend such action.

If the current wording and interpretation is preferred, with the very high standard it creates, FIPA recommends that penalties or presumption of liability should be added to s.25.

If the head of a public body, under a statutory requirement to release information in the public interest, fails to do so when health or safety of individuals is involved, the head should be made to pay a price.

This could be either in the form of a direct penalty, or it could be a statutory presumption of negligence and liability to those suffering damages as a result of the failure to release the information in the public interest.

FIPA recommends that s.25 be amended to take into account the ruling on public interest by the Supreme Court of Canada in *Grant v. Torstar Corp*.

[32] *Grant v. Torstar Corp*., 2009 SCC 61
[33] ibid, para 105
[34] ibid, para 106

In the alternative, FIPA recommends penalties be imposed on the head of a public body who does not release information where such release is found to be in the public interest as currently interpreted.

FIPA further recommends that the Commissioner should explicitly be given the power to apply this section and override decisions of public bodies to deny access.

7. Other matters

Out-of-scope

Section 4 (1) states that there is a general right of access to records. Section 4(2) states that this general right is subject to the exceptions set out in Part 2 of the Act, and s.4(3) says fees may be payable.

However, FIPA has run into repeated instances where public bodies have removed large parts of records on the grounds that they are "out of scope" of the request.

"Out of scope" is not an exception listed in Part 2 of the Act. Nor do officials ever state that the requested records are those listed in s.3 (1) of the Act as not being subject to the Act.

What this means is that officials have created their own unlimited new exception to the requirement to release records. This cannot be allowed to stand.

It may be argued that it is a matter of convenience for the requester. For example, a requested record may contain hundreds of pages, of which only a few appear to be related to what is being sought. If the entire records was to be reproduced, each page would have to be copied, then examined in detailed for possible exceptions, when it appears the requester is looking for a much more specific few pages. If that is the case, then the option should be with the REQUESTER to say they don't want more than certain pages released, or that they want the entire document and are willing to pay the fees associated with having the entire document reproduced and released.

What happens now leads to the suspicion that what is described as "out of scope" may be information the public body does not want to release, but cannot find any legal reason to withhold.

Regardless of the motivation, such a refusal to release is not authorized by law. As such it is a violation of s.4. The alternative is that it will eventually be challenged either before the Commissioner or in court, and none of us knows what they may decide.

FIPA recommends that section 3 be amended to prevent improper use of 'out of scope'.

Economic and business interests

As noted in the section on Information Laundering, it is vital that quangos and private service providers be made subject to the Act. However, this is subject to these bodies having protection under s.17 (economic interests of a public body) and s.21 (business interests of a third party). The harms-based tests in these sections have been clearly articulated by judicial interpretation and interpretation by the Commissioner and they strike the right balance between protection of legitimate economic interests and the public's right to know. In order for that balance to be maintained, the wording of these sections should not be changed, as any new language would doubtless result in uncertainty and probably expensive litigation.

FIPA recommends that Sections (17 and 21) not be altered.

Privacy protection

The BC government has come a long way in improving privacy protection in the province since 2001. It has shown strong leadership among the provinces, first by introducing the *Personal Information Protection Act* and second, by strengthening the privacy provisions of FOIPPA to counter the potential impact of foreign legislation when the personal information of British Columbians is disclosed to foreign owned corporations.

However, privacy protection continues to be a difficult issue in BC. These positive advances in privacy protection stand in stark contrast to a government project that will collect, use and disclose an unprecedented amount of citizens' personal information, not only across government ministries, but with other provinces, the federal government, and service delivery providers outside government.

The push for greater data collection and sharing brings us to the single most important challenge facing this committee and the government in improving the privacy part of the act: where to draw the line on what information and how much information about citizens is proper for government to collect, share and disclose, and for what purposes.

The danger here is the development of so-called "Big Brother" databases and networks such as the infamous Longitudinal Labour Force File within the federal Human Resources Development Corporation (HRDC) which linked an estimated 2000 separate pieces of information about citizens. When the existence of this database became public in 2000, it was dismantled after a huge national public outcry.

Although this salutary climbdown has been followed by a renewed government drive to collect and match information about individuals since 9/11, the dismantling of the HRDC Big Brother database has to some degree become a marker of where citizens do not want their governments to go in monitoring their citizens in a free society.

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 if can go further and share this information across government 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.[35]

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.36

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.

---

[35] *R. v. Dyment* [1988] 2 S.C.R. 417 ,
[36] *R.* v. *Plant*,[1993] 3 S.C.R. 281, para. 19 .

No 'Reasonableness' Standard in FOIPPA

Part 3 of FOIPPA, "Protection of Privacy", establishes the rules under which public bodies may collect, use, disclose and retain personal information. The rules are different for collection than for use, disclosure and retention, and they create a framework which enables widespread sharing of personal information by public bodies without any apparent standard of appropriateness or reasonableness.

While the standards imposed by FOIPPA might have been sufficient when information was held in electronic or paper "silos" in different Ministries, departments or agencies, it is now government policy to build a "citizen-centred" model to enable more efficient electronic sharing of citizens' personal information across the government as a whole. The explicit purpose of building these systems is to facilitate sharing for current and as-yet-unknown government programs.

In the past, we could rely on the principle of "practical obscurity" – information was inaccessible or obscured simply because as a practical matter, computer systems could not 'talk to each other' and paper records were often too voluminous and diffuse to enable the compilation of dossiers about citizens. Those days are gone.

Now our government has at its disposal a vast electronic storehouse of records which is now, or will soon be, searchable and shareable with remarkable ease. And with no objective standard for reasonableness or appropriateness against which to test a government program, there is a risk that new programs may spring up specifically for the purpose of using data that is already in the hands of government.

One example is called the "Social Sector Integrated Case Management Project." If this project comes to fruition, it will result in an unprecedented amount of data-sharing and data-matching across government ministries, and unprecedented scrutiny of the intimate details of individuals' lives by government officials.

To achieve the goals of the Integrated Case Management project, service delivery will need to be what is described as "collaborative and citizen-centred – not from one organization alone, but across the social sector":

> This will provide the holistic view of each citizen required to truly integrate delivery of social services in support of Great Goal 3, linking case information collected by other organizations delivering services to the public, such as the ministries of Health, Education, and the Attorney General, other provinces, the federal government, and Service Delivery Providers. [37]

[37] *Ministry of Employment and Income Assistance, Request for Proposals: Case Management Software* [RFP] SATP-239, November 6, 2007at p. 9

FOIPPA is unlikely to provide a bulwark against this vast invasion of privacy.

How to remedy the shortcomings in FOIPPA's Privacy Provisions

The primary purpose of the FOIPPA, set out in section 2, is to make public bodies more accountable. Another of the purposes of the FIOPPA is to "prevent the *unauthorized* collection, use and disclosure of personal information." But because there is no objective standard of reasonableness to which a government purpose for collection, use or disclosure must be measured, anything that is *authorized* is permitted under FOPPA, regardless of whether it is reasonable. And so the very purpose of FOIPPA – to make government more accountable - is not being met.

Privacy laws and principles, and citizen expectations around privacy, have advanced considerably since the last amendments to the FOIPPA. Citizens have become more sophisticated in their understanding of the implications of the collection, use and disclosure of their personal information and more skeptical about vague or overbroad frameworks which enable governments to share it in a potentially arbitrary manner. One of the reasons for this is the enactment of the province's *Personal Information Protection Act* (PIPA), which protects privacy in the provincially-regulated private sector.

PIPA establishes a minimum standard of reasonableness for any purpose for which personal information may be used by a private-sector organization: regardless of whether an individual has consented, the *purpose* for a collection, use or disclosure of personal information *must be* reasonable and appropriate in the circumstances.

Organizations have an additional threshold to meet when they wish to treat an individual's consent as having been implied for a specific purpose: the organization must take into account the sensitivity of the personal information in the circumstances.

No such standards are imposed on public bodies. Public bodies have no statutory duty to consider whether a particular use, or disclosure is reasonable, or appropriate in the circumstances and do not have to consider the sensitivity of the personal information except when addressing the duty to safeguard information.

The net effect of this is that public bodies are less accountable to individuals than organizations in the private sector, even though public bodies have much more power to collect, use and disclose highly sensitive information about individuals without their consent and very frequently without their knowledge.

There are two key provisions in FOIPPA which enable widespread sharing for virtually any purpose at any time.

Under section 32(a) personal information may be used

> (a) for a purpose for which it was obtained or compiled, or for a use consistent with that purpose;
>
> [and…]
>
> (c) for a purpose for which that information may be disclosed to that public body under sections 33 -36.

Use for a "consistent purpose" is a use that, pursuant to s. 34, "has a reasonable and direct connection to" the purpose for which the information was obtained or compiled and "is necessary for performing the statutory duties of, or for operating a legally authorized program of, the public body that uses or discloses the information or causes the information to be used or disclosed."

Section 33.2(d) provides that personal information may be disclosed to a public body or a Minister if necessary for the delivery of a "common or integrated program or activity

> s. 33.2(d) to an officer or employee of a public body or to a minister, if the information is necessary for the delivery of a common or integrated program or activity and for the performance of the duties of the officer, employee or minister to whom the information is disclosed.

These provisions are wide enough to permit almost any sharing among government bodies, provided that the new purpose has a "reasonable and direct connection" to the old purpose and the information is necessary, *or* the disclosure or use is for a "common or integrated activity."

This circularity means that government bodies have enormous latitude. *As long as the purpose of the new program or new use is reasonably and directly connected to the old purpose and the information is necessary for the new program or use, it can be used or disclosed, even if the purposes may have been wholly unimagined at the time the information is collected.*

Or, where there is a common or integrated program, the information may be used by a public body, regardless of whether the common or integrated program is the same "program or activity" for which the information was originally collected.

Data Sharing

The government cleared the way for very broad disclosures of personal information by public bodies when it added the following subsection to section 33 in 2002:

33 (f.1) permits disclosure of personal information as follows:

> to an officer or employee of a public body or to a minister, if the information is necessary for the delivery of a common or integrated program or activity and for the performance of the duties of the officer or employee or minister to whom the information is disclosed,

In our view, this amendment sets far too low a standard for information-sharing between government departments in the absence of the consent of the individual concerned.

Further, it is our view that section 33 (f) of the FOIPP Act, of which (f.1) is an extrapolation, also sets too low a standard. These subsections would (as an example) permit the disclosure of an individual's sensitive personal health information to an officer, employee or minister of government for performance of "duties". These duties may not be defined or specified in legislation, and the purpose may be completely different than originally intended. FIPA is of the view that this standard of disclosure falls far below what is now viewed as acceptable privacy practice.

Section 33(f) permits disclosure of personal information:

> to an officer or employee of the public body or to a minister, if the information is necessary for the performance of the duties of, or for the protection of the health or safety of, the officer, employee or minister,

FIPA recommends that data sharing be subject to approval of the Commissioner, as it is under the federal Privacy Act.[38]

Justification Principle

Any legislation that infringes citizens' rights must be reasonable and demonstrably justified and the onus of proving that a limitation meets that criteria is on the party seeking to uphold the limitation.[39] As discussed in *R. v. Oakes* two criteria must be met:

(1) The objective of the legislation must be sufficiently important, pressing and substantial, "to warrant overriding a constitutionally-protected right"; and

(2) The means chosen must be reasonable, demonstrably justified, and proportional, balancing the interests of society with those of the individuals. With respect to proportionality, the measures must be "rationally connected to the objective", and impair the right "as little as possible". Further, "there must be a proportionality between the effects of the measures… and the objective".

[38] Privacy Act (R.S., 1985, c. P-21) s.9(4)
[39] *R. v. Oakes* [1986] 1 SCR 103

We agree with the Privacy Commissioner of Canada that any proposal that seeks to limit the right to privacy must meet a four-part test:

- it must be demonstrably necessary in order to meet some specific need;
- it must be demonstrably likely to be effective in achieving its intended purpose. In other words, it must be likely to actually make us significantly safer, not just make us feel safer;
- the intrusion on privacy must be proportional to the security benefit to be derived; and
- it must be demonstrable that no other, less privacy-intrusive, measure would suffice to achieve the same purpose.[40]

To strengthen the Act's privacy protections, FIPA recommends that:

the privacy impact of programs and practices should be measured against a legislative yardstick such as a privacy charter. If not justifiable, they should be modified or abandoned.[41]

access to personal information be further limited and particularized by upgrading sections 32, 33 and 34 to meet the higher standards embodied in PIPEDA and PIPA.

in particular, the definitions of "consistent use" "collection" and "disclosure" are too broad and should be amended. Section 34 should be amended to provide that the purpose of a use or disclosure of personal information is a consistent purpose only if a person might reasonably have expected such a use or disclosure[42]

section 71 should be amended to require public bodies to make personal information available to the individual without charge, with limited exceptions for costly records as X-rays and other special cases.[43]

the Act be amended to include privacy protection requirements for subsequent handling of personal information when it is released to

---

[40] Letter to the Ministers responsible for the "Lawful Access" proposals, November 25, 2002. http://privcom.gc.ca/media/le_021125_e.asp

[41] OIPC Recommendation 10: The Act should be amended to require public bodies to consider, as part of any assessment respecting the privacy impact of a law, policy, program or technology under consideration, with that assessment being conducted according to a privacy charter incorporated in the Act or enacted as a free-standing statute. Where the privacy impacts cannot be minimized to an acceptable level, the proposal should be abandoned.

[42] See Freedom of Information and Protection of Privacy Act, R.S.O. 1990, c. F.31, s. 43

[43] See Special Committee recommendation no. 26 and recommendation no. 1, Information and Privacy Commissioner.

third parties (e.g. employers in cases before the Worker's Compensation Board), and

the Act be amended to clearly extend to government services that are privatized or contracted out, and when personal information is given to non-government organizations.

* * *

Conclusion

This Committee's predecessors reviewed this Act in 2004 and came to a strong conclusion that a number of changes were necessary. The changes they recommended were needed in 2004 and they are desperately needed in 2010.

We urge you to consider carefully the recommendations we have brought before you. However, if you do not see fit to act in the manner we recommend, we urge that you at least insist on government action on the remaining recommendations still undone from the 2004 committee.

The people of BC are counting on you to ensure that their right to freedom of information and privacy are preserved and protected.

Summary of Recommendations

FIPA recommends that:

1. **A new s.2(3) be added to require the use of information technology to advance the purposes of the Act, particularly the routine release of information.**

2. **The protections provided to whistleblowers should be set out in law, probably in a separate law as exists at the federal level.**

3. **A positive duty to create and maintain records be incorporated into the FOIPP Act or other legislation – a duty to record decision-making, and minimum requirements for record keeping in critical areas.**

4. **A section be incorporated into the FOIPP Act to penalize any person or public body that deliberately destroys documents against the authority of the FOIPP Act and the Document Disposal Act.**

5. **FOIPPA be amended to provide for penalties for heads of public bodies who flagrantly breach the duty to assist.**

6. **S.20(3) be amended to provide for immediate release of all requested records to the requester if the records in question are not made public after the 60 day period.**

7. **S.75(5.1) be amended to clarify that a fee waiver can be requested as part of the request for information.**

8. **An automatic fee waiver for non-compliance be implemented.**

9. **Section 11 of the Act should be amended to eliminate the 20 day transfer period for public bodies which are part of the new FOI request system.**

10. **The FOIPP Act be extended to all public and quasi-public bodies and to records created by or in the custody or control of alternate service providers.**

11. **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)

12. 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.

13. S.25 be amended to take into account the ruling on public interest by the Supreme Court of Canada in *Grant v. Torstar Corp*.

In the alternative, penalties be imposed on the head of a public body who does not release information where such release is found to be in the public interest as currently interpreted.

The Commissioner should explicitly be given the power to apply this section and override decisions of public bodies to deny access.

14. Section 3 be amended to prevent improper use of 'out of scope'.

15. Sections 17 and 21 not be altered.

16. Data sharing be subject to approval of the Commissioner, as it is under the federal Privacy Act.

17. The privacy impact of programs and practices should be measured against a legislative yardstick such as a privacy charter. If not justifiable, they should be modified or abandoned.

18. Access to personal information be further limited and particularized by upgrading sections 32, 33 and 34 to meet the higher standards embodied in PIPEDA and PIPA. In particular, the definitions of "consistent use" "collection" and "disclosure" are too broad and should be amended. Section 34 should be amended to provide that the purpose of a use or disclosure of personal information is a consistent purpose only if a person might reasonably have expected such a use or disclosure.

19. Section 71 be amended to require public bodies to make personal information available to the individual without charge, with limited exceptions for costly records as X-rays and other special cases.

20. The Act should be amended to include privacy protection requirements for subsequent handling of personal information when it is released to third parties (e.g. employers in cases before the Worker's Compensation Board), and that the Act be amended to clearly extend to government services that are privatized or contracted out, and when personal information is given to non-government organizations.

Appendix 1

The analysis of 'advice or recommendations' most commonly used by various jurisdictions across this country, and in British Columbia until 2002 is as follows.

First, the record must be examined to determine whether the information it contains qualifies as advice or recommendations. In order to qualify as "advice or recommendations", the information in the record must suggest a course of action that will ultimately be accepted or rejected by the person being advised.[44]

Second, the record must be examined to see if it reveals advice or recommendations. Advice or recommendations may be revealed in two ways:

- the information itself consists of advice or recommendations, or

- the information, if disclosed, would permit one to accurately infer the advice or recommendations given.[45]

Finally, the information must be examined to see if it falls within the scope of one of the mandatory release subsections of s.13(2).[46]

---

[44] [Orders PO-2028, PO-2084, upheld on judicial review in *Ontario (Ministry of Northern Development and Mines) v. Ontario (Assistant Information and Privacy Commissioner)*, [2004] O.J. No. 163 (Div. Ct.), aff'd [2005] O.J. No. 4048 (C.A.), leave to appeal refused [2006] S.C.C.A. No. 564; see also *Ontario (Ministry of Transportation) v. Ontario (Information and Privacy Commissioner)*, [2005] O.J. No. 4047 (C.A.), leave to appeal refused [2006] S.C.C.A. No. 563].

[45] [Orders PO-2028, PO-2084, upheld on judicial review in *Ontario (Ministry of Northern Development and Mines) v. Ontario (Assistant Information and Privacy Commissioner)*, [2004]
[IPC Order MO-2066/June 30, 2006] O.J. No. 163 (Div. Ct.), aff'd [2005] O.J. No. 4048 (C.A.), leave to appeal refused [2006] S.C.C.A. No. 564; see also *Ontario (Ministry of Transportation) v. Ontario (Information and Privacy Commissioner)*, [2005] O.J. No. 4047 (C.A.), leave to appeal refused [2006] S.C.C.A. No. 563]

[46] [Order P-434; Order PO-1993, upheld on judicial review in *Ontario (Ministry of Transportation) v. Ontario (Information and Privacy Commissioner)*, [2004] O.J. No. 224 (Div. Ct.), aff'd [2005] O.J. No. 4047 (C.A.), leave to appeal refused [2005] S.C.C.A. No. 563; Order PO-2115; Order P-363, upheld on judicial review in *Ontario (Human Rights Commission) v. Ontario (Information and Privacy Commissioner)* (March 25, 1994), Toronto Doc. 721/92 (Ont. Div. Ct.); Order PO-2028, upheld on judicial review in *Ontario (Ministry of Northern Development and Mines) v. Ontario (Assistant Information and Privacy Commissioner)*, [2004] O.J. No. 163 (Div. Ct.), aff'd [2005] O.J. No. 4048 (C.A.), leave to appeal refused [2005] S.C.C.A. No. 564]

Examples of the types of information that have been found not to qualify as advice or recommendations include

- factual or background information
- analytical information
- evaluative information
- notifications or cautions
- views
- draft documents
- a supervisor's direction to staff on how to conduct an investigation

Appendix 2

FAILING FOI: How the BC Government flouts the Freedom of Information Act and stonewalls FOI requests, FIPA, May 2009

Available at http://fipa.bc.ca/library/Reports_and_Submissions/Failing_FOI-May_2009-FINAL.pdf

Appendix 3

A Prescription for "Dr. Doe": Proposed Revisions to s. 13 of the* Freedom of Information and Protection of Privacy Act *in Response to the Decision in College of Physicians of British Columbia v. British Columbia (Information and Privacy Commissioner)

Available at http://fipa.bc.ca/library/Reports_and_Submissions/A_Prescription_for_Dr_Doe-Jan_2004.pdf