Page 001 to/à Page 003

Withheld pursuant to/removed as

s.13

ADVICE TO MINISTER
ESTIMATES NOTE
FEBRUARY 18, 2016

ISSUE: SUBSIDIARY CORPORATIONS UNDER THE *FREEDOM OF INFORMATION AND PRIVACY ACT* (FOIPPA)

s.13

CURRENT STATUS:

- s.13
-
-

KEY FACTS REGARDING THE ISSUE:

On October 20, 2011, the Minister responsible for FOIPPA received a letter from the OIPC asking the ministry to draft amendments to FOIPPA to ensure coverage of subsidiary corporations of local public bodies. The Commissioner made this request in response to a 2009 BC Supreme Court decision (Simon Fraser University (SFU) v. British Columbia (Information and Privacy Commissioner), 2009 BCSC 1481) which held that FOIPPA did not extend to the records of SFU's subsidiary corporations.

The 2010 Special Committee that reviewed FOIPPA made a similar, but slightly broader, recommendation to expand the definition of “public body” in Schedule 1 to include any corporation that is created or owned by a public body, including an educational body. s.13
s.13

ADVICE TO MINISTER
ESTIMATES NOTE

Contact:	Sharon Plater	250 356-0322
File Created:	February 18, 2016	
File Updated:		
File Location:		

Ministry of Finance

BRIEFING DOCUMENT

To:	Honourable Michael de Jong, Q.C. Minister of Finance	**Date Requested:**	Dec 12, 2015
		Date Required:	Dec 29, 2015
Initiated by:	Privacy and Legislation Branch		
		Date Prepared:	Dec 18, 2015
Ministry Contact:	Sharon Plater	**Phone Number:**	(250) 356-0322
		Email:	Sharon.Plater@gov.bc.ca
		Cliff #:	

TITLE: Special Committee to Review the Freedom of Information and Protection of Privacy Act – Status Update

---

PURPOSE: FOR INFORMATION

COMMENTS: A Special Committee to review the Freedom of Information and Protection of Privacy Act was struck in May. The Committee is currently accepting submissions from stakeholders and will be producing a report with recommendations for changes to FOIPPA in spring 2016.

BACKGROUND:

The Freedom of Information and Protection of Privacy Act (FOIPPA), British Columbia's public sector privacy legislation, was passed in June of 1992 and came into force for provincial government public bodies in October 1993. FOIPPA applies to all pubic bodies in BC and governs the collection, use and disclosure of personal information by the public sector.

Section 80 of FOIPPA states that at least once every six years, a Special Committee of the Legislative Assembly must be appointed and undertake a comprehensive review of the Act. The most recent Special Committee was struck on May 27, 2015 and has received submissions during the current consultation period from government, the Office of the Information and Privacy Commissioner (OIPC) and other stakeholders. Once the consultation period has ended, on January 29, the Special Committee will have until May 27th to submit a report of its review to the Legislative Assembly, which will include recommendations for changes to the Act.

DISCUSSION:

The OIPC presented to the Special Committee and provided their written submission on November 18th. While the Commissioner made several recommendations both in her presentation and in the written submission, the following selection is noteworthy, and may have a significant impact to government:

s.13

As part of the consultations conducted by the Special Committee, stakeholders from the public and private sector, as well as interested citizens, were invited to present during four scheduled public hearings, which took place in October and November. In addition, the Special Committee will continue to accept written submissions up until the January deadline.

Among the wide range of stakeholders who have participated in the public consultation, the Special Committee has heard from the BC Freedom of Information and Privacy Association, the Centre for Law and Democracy, Vancouver Coastal Health Authority

and members of the media. Though the Special Committee received presentations on a myriad of topics, covering privacy, access, records management and government processes, the following issues were discussed in depth:

- The inclusion of subsidiary corporations in FOIPPA
- Elimination of access fees
- Data residency
- The inclusion of a legislated duty to document key actions and decisions
- Expansion of the "public interest" disclosure provision

On November 18th, Government Chief Information Officer, Bette-Jo Hughes, also presented to the Special Committee on behalf of government. This presentation dealt largely with:

- Data residency
- Harmonization with global privacy standards
- The increasing proliferation of records in a digital age
- Availability and impact of metadata
- Access through proactive disclosure
- Government's Privacy Management and Accountability Policy
- Proposed changes to FOIPPA

s.13

As stated above, the next milestone in the Special Committee process will be the culmination of the consultation period on January 29th. Once completed, the Special Committee will prepare their report, including a list of recommendations which are expected to echo those of the Commissioner. This has been typical of past Special Committees and is anticipated for this year as well.

Subsidiary Corporations of Local Public Bodies

KEY MESSAGES

- **Ariel 14, 1 ½ line spacing, bold**
- **Maximum ½ page**
- **To be completed by GCPE**

KEY POINTS AND BACKGROUND

- On October 20, 2011, the Minister received a letter from the Information and Privacy Commissioner asking the ministry to draft amendments to the *Freedom of Information and Protection of Privacy Act* (FOIPPA) to ensure coverage of subsidiary corporations of local public bodies.
- The Commissioner made this request in response to a 2009 BC Supreme Court decision *(Simon Fraser University v. British Columbia (Information and Privacy Commissioner), 2009 BCSC 1481)* which held that the FOIPPA did not extend to the records of subsidiary corporations owned by Simon Fraser University.
- The 2010 Special Committee that reviewed FOIPPA made a similar, but slightly broader, recommendation (#4) to: expand the definition of "public body" in Schedule 1 to include any corporation that is created or owned by a public body, including an educational body.
- Currently, corporations that are created or owned by "local government bodies" (which include municipalities and regional districts) are, by definition, already covered by FOIPPA.
- However, this is not the case for corporations created or owned by universities, school boards, health authorities and other types of "local public bodies". These corporations are not, by definition, covered by the Act.
- Government has consulted with public bodies such as universities and school boards to understand the scope of the issue and the impact of covering these public bodies' corporations.

- Consultations have indicated that this is a complex issue due to the divergent types of corporations that are affiliated with local public bodies. Further review and consideration is required.

- Government will be identifying and reviewing the options for extending coverage of the FOIPPA to subsidiary corporations of local public bodies once the scope of the issue and the impact of adding these corporations is fully understood.

- A question is often asked about the 2006 Ministry of Education commitment that school district business companies comply with the *Freedom of Information and Protection of Privacy Act.* While the ministry made changes to the *School Act* in 2007, enabling school boards to create business entities that could generate extra funds for the districts it decided not to add school district business companies to coverage of FOIPPA and chose instead to achieve the accountability goals in other ways.

From:	Reed, Matt MTIC:EX
To:	Plater, Carmelina MTIC:EX
Cc:	Lowe, Charmaine MTIC:EX
Subject:	subcorps
Date:	Thursday, January 14, 2016 8:52:48 AM
Attachments:	SubCorps IN.doc

Hi Carm,
Mark mentioned that you were looking for materials on sub corps. Here is a draft on an IN on the topic.
Let me know if you have any questions.
Thanks,
-m

Matt Reed
Director, Strategic Privacy
250 514-8870

Ministry of Finance

BRIEFING DOCUMENT

To: Honourable Michael de Jong, Q.C.
Minister of Finance

Date Requested:
Date Required:

Initiated by:

Date Prepared:

Ministry Contact:

Phone Number:
Email:

Cliff #:

TITLE: Subsidiary corporations under the *Freedom of Information and Protection of Privacy Act* (FOIPPA).

PURPOSE:
(X) FOR INFORMATION

DATE PREPARED: December 23rd, 2015

TITLE: Subsidiary corporations under the *Freedom of Information and Protection of Privacy Act* (FOIPPA).

ISSUE: Subsidiary corporations of ministries and most other public bodies are not subject to FOIPPA, as was recommend by the OIPC.

BACKGROUND:

On October 20, 2011, the Minister responsible for FOIPPA received a letter from the Office of the Information and Privacy Commissioner (OIPC) asking the ministry to draft amendments to FOIPPA to ensure coverage of subsidiary corporations of local public bodies. The Commissioner made this request in response to a 2009 BC Supreme Court decision (Simon Fraser University (SFU) v. British Columbia (Information and Privacy Commissioner), 2009 BCSC 1481) which held that FOIPPA did not extend to the records of SFU's subsidiary corporations.

The 2010 Special Committee that reviewed FOIPPA made a similar, but slightly broader, recommendation to: expand the definition of "public body" in Schedule 1 to include any corporation that is created or owned by a public body, including an educational body. The 2015 Special Committee has shown significant and sustained interest in the issue of subsidiary corporations. Similarly, the OIPC's submission to the Special Committee recommended that subsidiary corporations of all public bodies be subject to FOIPPA, which is an expansion on her earlier recommendation.

Currently, corporations that are created or owned by "local government bodies" (which include municipalities and regional districts) are, by definition, already covered by FOIPPA. However, this is not the case for corporations created or owned by ministries, crowns, universities, school boards, health authorities, and other types of "local public bodies". These corporations are not, by definition, covered by the Act.

Government has consulted with ministries, crowns, universities and school boards to understand the scope of the issue and the impact of covering these public bodies' corporations. Consultations have indicated that this is a complex issue due to the divergent types of corporations that are affiliated with local public bodies.

DISCUSSION:

s.13

s.13

2015 OIPC Recommendations to the FOIPPA Special Committee

Recommendation	New / Previously Recommended by OIPC	Current Position	Analysis / Implications
Key OIPC Recommendations			
1. Add to Part 2 of FIPPA a duty for public bodies to document key actions and decisions based on the definition of government information" in the Information Management Act.	**Previously recommended**	s.13	
2. Amend FIPPA to move paragraph (n) of the definition of "local government body" into the definition of "public body" in Schedule I, so that entities such as subsidiaries of educational bodies and the BCACP fall within the scope of FIPPA.	**Previously recommended**		

Recommendation	New / Previously Recommended by OIPC	Current Position	Analysis / Implications
			that Powerex and other such entities would be covered.
3. Add to Part 3 of FIPPA a breach notification and reporting framework which includes: **• A definition of a privacy breach: includes the loss of, unauthorized access to or unauthorized collection, use, disclosure or disposal of personal information.** **• A requirement to notify individuals when their personal information is affected by a known or suspected breach, if the breach could reasonably be expected to cause significant harm to the individual.** **• A requirement that a public body report to the Commissioner any breach involving personal information under the custody or control of that public body, if the breach or suspected breach could reasonably be expected to cause harm to an individual and/or involves a large number of individuals;** **• A timing requirement that process of notification and reporting must begin without unreasonable delay once a breach is discovered;** **• Authority for the Commissioner to order notification to an individual affected by a breach; and** **• A requirement that public bodies document privacy breaches and decisions about notification and reporting.**	**Previously recommended**	s.13	

Recommendation	New / Previously Recommended by OIPC	Current Position	Analysis / Implications
4. Amend s. 42 of FIPPA to expand the Commissioner's oversight by granting the Commissioner the jurisdiction to review matters or allegations of unauthorized destruction of records. **The Commissioner should have jurisdiction over the unauthorized destruction of records as set out in:** **• any enactment of British Columbia, or** **• set out in a bylaw, resolution or other legal instrument by which a local public body acts or, if a local public body does not have a bylaw, resolution or other legal instrument setting out rules related to the destruction of records, as authorized by the governing body of a local public body.** **The oversight over unauthorized destruction should come with complementary offences and penalties under FIPPA.**	**New**	s.13	
5. Amend FIPPA to require public bodies to ensure that the name and type of applicant is only disclosed to the individual at the public body that receives an access request on behalf of that public body, while providing for limited exceptions where the applicant is requesting their own personal information or where the name of the applicant is necessary to respond to the request.	**Previously recommended**		

Recommendation	New / Previously Recommended by OIPC	Current Position	Analysis / Implications
6. Penalties for offences committed by individuals under FIPPA should be raised to be up to a maximum of $50,000 for both general and privacy offences.	**New**	s.13	
7. Add a privacy protection offence to s. 74.1 that makes it an offence to collect, use, or disclosure personal information in contravention of Part 3 of FIPPA.	**New**		
8. Add to s. 29 of FIPPA a requirement that public bodies correct personal information when an individual requests that his or her personal information be corrected if the public body is satisfied on reasonable grounds that the request made should be implemented.	**New**		
9. Section 13(1) of FIPPA should be amended to clarify the following: **• "advice" and "recommendations" are similar and often interchangeably used terms, rather than sweeping and separate concepts;** **• "advice" or "recommendations" set out suggested actions for acceptance or rejection during a deliberative process;** **• the "advice" or "recommendations" does not apply to the facts upon which the advice**	**Previously recommended**		

Recommendation	New / Previously Recommended by OIPC	Current Position	Analysis / Implications
or recommendation is based; and **• the "advice" or "recommendations" does not apply to factual, investigative, or background material, for the assessment or analysis of such material, or for professional or technical opinions.**		s.13	
10. Amend ss. 71 and 71.1 of FIPPA to require the publication of any categories of records that are established by the head of a public body or the Minister and made available to the public without an access request. This list should include links to relevant information or records.	New		
11. Add an exception to s. 33.1(1) that states that a public body may disclose personal information inside or outside of Canada, if the information is contained in a non-statutory investigation or fact-finding report commissioned by a public body, where the head of the public body concludes the public interest in disclosure outweighs the privacy	New		

Recommendation	New / Previously Recommended by OIPC	Current Position	Analysis / Implications
interests of any person whose personal information is contained in the report.		s.13	
12. Add to FIPPA a requirement that public bodies have a privacy management program that: • designates one or more individuals to be responsible for ensuring that the public body complies with FIPPA; • is tailored to the structure, scale, volume, and sensitivity of the personal information collected by the public body; • includes policies and practices that are developed and followed so that the public body can meet its obligations under FIPPA, and makes policies publicly available; • includes privacy training for employees of the public body; • has a process to respond to complaints that may arise respecting the application of FIPPA; and • is regularly monitored and updated.	New		
13. Add a de-identification requirement to s. 33.2(I) of FIPPA for any personal information that is disclosed for the purposes of planning or evaluating a program or activity of a public body.	New		
14. That FIPPA be amended to limit the exemption in s. 3(J)(e) to Part 2 of FIPPA.	**New**		

Recommendation	New / Previously Recommended by OIPC	Current Position	Analysis / Implications
15. Amend the definition for "data-linking" in Schedule I of FIPPA to define data-linking as the linking or combining of data sets where the purpose of linking or combining the information is different from the original purpose for which the information in at least one of the data sets that was originally obtained or compiled, and any purposes consistent with that original purpose.	**Previously recommended**	s.13	
16. Repeal s. 36.1(2) of FIPPA to remove the exemption of the health care sector from the data-linking oversight provisions of the Act.	Previously recommended		
17. Amend Part 6 of FIPPA to require government to list provisions in statutes that prevail over FIPPA in a schedule to the Act, and amend s. 80 of FIPPA to include a review of those provisions as part of the statutory review of the Act.	New		
18. Amend s. 56 of FIPPA to permit the Commissioner to extend the 90 day time limit to review requests in a manner that is consistent with s. 50(8) of PIPA**.**	**Previously recommended**		
19. Amend parts 4 and 5 of FIPPA to combine the complaint process and the review and inquiry process into a unitary process for the Commissioner to investigate, review, mediate, inquire into and make orders about complaints respecting decisions under FIPPA or other allegations of non compliance with FIPPA.	**Previously recommended**		

Recommendation	New / Previously Recommended by OIPC	Current Position	Analysis / Implications
20. Government should enact new comprehensive health information privacy legislation at the earliest opportunity.	New	s.13	
21. Amend section 80 (1) of FIPPA to change the review cycle from 6 years to every 3-4 years.	New		

From:	Reed, Matt MTIC:EX
To:	Plater, Sharon MTIC:EX
Cc:	Begley, Rhianna MTIC:EX
Subject:	BN - FOIPPA Special Committee (2)
Date:	Thursday, March 3, 2016 3:30:58 PM
Attachments:	BN - FOIPPA Special Committee (2).doc

Hi Sharon,
As requested, here is the BN on the special committee submission recommendations that would present serious issues. The content around other key issues has been added so that it flows more intuitively.
Happy to make any changes.
Thanks,
-m

Ministry of Finance

BRIEFING DOCUMENT

To:		**Date Requested:**	
		Date Required:	
Initiated by:	Privacy, Compliance and Training Branch		
		Date Prepared:	March 1, 2016
Ministry Contact:	Sharon Plater	**Phone Number:**	(250) 356-0322
		Email:	Sharon.Plater@gov.bc.ca
		Cliff #:	

TITLE: Special Committee to Review the Freedom of Information and Protection of Privacy Act

---

PURPOSE: FOR INFORMATION

COMMENTS: A Special Committee to review the Freedom of Information and Protection of Privacy Act was struck in May 2015. The Committee received submissions until January 29, 2016. The Committee will produce a report of recommendations by May 27, 2016.

BACKGROUND:

The Freedom of Information and Protection of Privacy Act (FOIPPA), British Columbia's public sector privacy legislation, was passed in June of 1992 and came into force for provincial government public bodies in October 1993. FOIPPA applies to all pubic bodies in BC and governs the collection, use and disclosure of personal information by the public sector.

Section 80 of FOIPPA states that at least once every six years, a Special Committee of the Legislative Assembly must be appointed to undertake a comprehensive review of the Act. The most recent Special Committee was struck on May 27, 2015 and has received submissions from government, the Office of the Information and Privacy Commissioner (OIPC) and other stakeholders from the public and private sector, as well as interested citizens. The consultation period ended on January 29, 2016. The Special Committee has until May 27, 2016 to submit a report of its review to the Legislative Assembly, which will include recommendations for changes to the Act.

Among the wide range of stakeholders who have participated in the public consultation, the Special Committee has heard from the BC Freedom of Information and Privacy Association, the Centre for Law and Democracy, BC Civil Liberties Association, the Research Universities Council of British Columbia, a number of the Health Authorities, TransLink, ICBC and members of the media. Though the Special Committee received presentations on a myriad of topics, covering privacy, access, records management and government processes, the following issues received significant attention from a variety of stakeholders. These issues include:

- Impose penalties on public bodies and/or public servants for contravening FOIPPA.

- Amend data residency provisions to allow public bodies to leverage technology solutions where data moves outsides of Canada.

- Address the issue of FOIPPA coverage for subsidiary corporations

- Implement a "duty to document" that would compel government to document key actions and decisions.

- Inclusion of a mandatory breach reporting requirement

- There are a number of submissions that seek to limit the coverage of various exemptions to disclosure (section 12, section 13 and section 14). Conversely, a number of submissions argued for an expansion of coverage (section 13, section 14, section 15, section 17 and section 21).

- A number of stakeholders spoke in favor of the OIPC's recent interpretation of section 25, which removes the element of temporal urgency when considering

disclosure in the public interest. In addition, some stakeholders recommended that this provision be amended to expand its application.

- There were a number of submissions that spoke to the need to make changes to improve access to information, including; amending provisions related to fees, timelines and the public body's duty to assist the applicant.

- The OIPC has called for amendments to section 42 of FOIPPA to expand the Commissioner's oversight by granting the Commissioner the jurisdiction to review matters or allegations of unauthorized destruction of records.

- A small subset of submissions called for an amendment that would allow for the reporting of abortion statistics (section 22.1)

DISCUSSION:

s.13

Freedom of Information and Protection of Privacy Act (FOIPP Act)
Special Committee (S.C.) to Review the FOIPP Act (2010)

Disposition of Recommendations
(March 30, 2011)

Rec. #	Recommendation	Analysis	Repeat Recommendations from the 20 already addressed from 2004	Repeat Recommendations from the 8 in 2004 still under consideration	Alignment with Special Committee submission, 3-year legislative plan and e-government plan	Disposition
Part 1 – Introductory Provisions:						
1	Add a new section 2(3) to acknowledge that information technology plays an important role in achieving the dual purposes of the Act by facilitating the routine disclosure of general information as well as enhancing safeguards for privacy protection.	s.13	Yes – 2004 (#2) Slightly different wording but same intent. The 2004 recommendation was addressed in part through new Routine Release Policy.		s.13	Policy – nothing further has been implemented.
2	Add a new section 2(4) to require that for an infringement of the right to privacy to be lawful, it must be proportional to the public interest that is achieved.					s.13

Rec. #	Recommendation	Analysis	Repeat Recommendations from the 20 already addressed from 2004	Repeat Recommendations from the 8 in 2004 still under consideration	Alignment with Special Committee submission, 3-year legislative plan and e-government plan	Disposition
3	Include the British Columbia Society for the Prevention of Cruelty to Animals by using definition (b) of *public body* in Schedule 1 that makes provision for adding an "other body" by regulation to Schedule 2; and add the proviso that access rights pertain only to those records that relate to this Society's statutory powers.	The SPCA is a not-for-profit society that acts in part under the *Prevention of Cruelty to Animals Act*.The majority of its operations and financial resources are not related to these responsibilities, however, the apprehension of animals and related activities are probably the most contentious.	Yes – 2004 (#3) A slightly different SPCA recommendation but with the same intent. It requested government to investigate why the SPCA had dual status as a not-for-profit and a public body and to consider whether it should be covered under the FOIPP Act. s.13 s.13		Not related	s.13
4	Expand the definition of "public body" in Schedule 1 to include any corporation that is created or owned by a public body, including	s.13			Not related	s.13

Rec. #	Recommendation	Analysis	Repeat Recommendations from the 20 already addressed from 2004	Repeat Recommendations from the 8 in 2004 still under consideration	Alignment with Special Committee submission, 3-year legislative plan and e-government plan	Disposition
	an educational body.	s.13				
5	Amend Section 3 to clarify that records created by or in the custody of a service-provider under contract to a public body are under the control of the public body on whose behalf the contractor provides services.	Part 3 of the Act, which are the privacy provisions, already brings the records of contractors that relate to a contract they hold for government under cover of the FOIPP Act. In addition, all contracts that involve personal information have access provisions in place. This would formalize what is already in place in most cases.	Yes – 2004 (#4) Being addressed in part through policy		Not related	Addressed in 2011 amendments.
6	Amend section 3(1)(e) by replacing “employees” with “faculty members and teaching support staff” of a post-secondary educational body.	Minor housekeeping clarification. No related issues.			Not related	Addressed in 2011 amendments.
7	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 Information and Privacy Commissioner for the routine	s.13	Yes – 2004 (#5) Addressed in part through updated Routine Release Policy.		s.13	Policy – no further implementation.

Ministry of Finance

BRIEFING DOCUMENT

To:	Athana Mentzelopoulos Deputy Minister	**Date Requested:** March 22, 2016 **Date Required:**	
Initiated by:	David Curtis ADM, Corporate Information and Records Management Office	**Date Prepared:**	March 22, 2016
Ministry Contact:		**Phone Number:** **Email:**	
		Cliff #:	

TITLE: Deputy Minister Meeting with Information and Privacy Commissioner

---

PURPOSE:

(X) FOR INFORMATION

COMMENTS:

Optional. Two or three sentences which put the issue into context.

Executive Director approval: _____ ADM approval: _____

DATE PREPARED: March 22, 2016

TITLE: Deputy Minister Meeting with Information and Privacy Commissioner

ISSUE: March 29, 2016 Meeting with Elizabeth Denham, Information and Privacy Commissioner

BACKGROUND:

An introductory lunch meeting has been scheduled for March 29, 2016, for Deputy Minister of Finance, Athana Mentzelopoulos, and Information and Privacy Commissioner (Commissioner), Elizabeth Denham. Deputy Attorney General, Richard Fyfe will also be attending.

s.13

The Commissioner is an independent officer of the Legislature with responsibility, under the *Freedom of Information and Protection of Privacy Act* (FOIPPA), for monitoring how the Act is administered and ensuring that its freedom of information and protection of privacy purposes are achieved. An overview of FOIPPA is attached as **Appendix 1**.

Commissioner Denham is British Columbia's third Information and Privacy Commissioner and was appointed in May 2010 for a six year term. Her term is due to end July 6, 2016 and she will not be seeking reappointment. She confirmed this in a letter to the Minister of Finance, dated March 22, 2016, where she informed the Minister that she had accepted the position as the Information Commissioner for the UK.

The Commissioner also has review and oversight responsibility under the *Personal Information Protection Act* (PIPA), British Columbia's private sector privacy legislation. An overview of PIPA is attached as **Appendix 2**.

The Commissioner does not have statutory responsibilities under government's *Document Disposal Act* (DDA), or the *Information Management Act* (IMA) which will replace the DDA once it is brought into force this Spring. However, as a former archivist she has a keen interest in records management and has made several recommendations to government on how it should improve its records management practices and oversight. The Commissioner was consulted on the development of the IMA and made, and continues to make, recommendations that would provide her office with some oversight over the IMA, specifically with respect to the destruction of records. An overview of the IMA is attached as **Appendix 3**.

DISCUSSION:

s.13

***Freedom of Information and Protection of Privacy Act* (FOIPPA)**
There is currently a Special Committee of the Legislature reviewing FOIPPA. In her submission to the Committee the Commissioner made a number of recommendations for legislative change.

Duty to Document
Commissioner Denham has recommended that government legislate a "duty to document" key decisions and actions. While she previously supported the inclusion of a "duty to document" in the IMA, she is now advocating for its inclusion in FOIPPA due to its broader scope and independent oversight. s.13
s.13

Subsidiary Corporations
A longstanding issue for the Commissioner, one that she has recommended more than once is the inclusion of subsidiary corporations of public bodies under FOIPPA. The current amendment proposed by the Commissioner proposes that the definition of public body be broadened to include all boards agencies, committees, commissions, panels and agencies in addition to corporations that are created or owned by a public body. s.13
s.13

Privacy Breach Notification and Privacy Management Programs
The Commissioner has also proposed amendments to FOIPPA that would make privacy breach notification and privacy management programs mandatory for all public bodies. Government currently provides monthly reports to the OIPC about each privacy incident investigated by government and reports all "serious" privacy breaches directly to the Commissioner. Government has also recently issued a corporate Privacy Management Accountability Policy (PMAP). s.13
s.13

Oversight over the Unauthorized Destruction of Records
The Commissioner has recommended that FOIPPA be amended to give her oversight over unauthorized destruction of records as set out in any enactment in British Columbia, or any legal instrument that is used by a local public body, as well as the associated offences and penalties. s.13
s.13

The destruction of records is currently governed by the *Document Disposal Act*, and going forward will be covered by the *Information Management Act*. The CRO is the statutory officer that has oversight authority over the IMA. Government is expanding its existing compliance program and implementing strong oversight through policy and practice improvement. s.13
s.13

s.13 For a complete list of the Commissioners recommendations to the Special Committee please see **Appendix 4**.

***Personal Information Protection Act* (PIPA)**
On February 17, 2016 the Commissioner wrote to the Deputy Minister of Finance and the Deputy Attorney General, making an urgent request that the Ministry of Finance sponsor a provision in a Miscellaneous Statutes Amendment, in the current legislative session, to repeal a subsection of the *Personal Information Protection Act* (PIPA).

The Commissioner is concerned that a recent interpretation of PIPA, made by the federal privacy commissioner will not allow for the generally accepted practice of `concurrent jurisdiction` in privacy cases involving inter-provincial commercial activities.

According to the B.C Commissioner, the federal commissioner has sited that a subsection of PIPA does not allow the federal office to share personal information with the B.C. Commissioner about cases that involve both the federal and B.C. jurisdictions.
s.13 .

Attachments

From:	Biggs, Jackie FIN:EX
To:	Plater, Sharon MTIC:EX
Subject:	FW: FOIPPA Special Committee (2)
Date:	Monday, April 18, 2016 12:45:06 PM
Attachments:	FOIPPA Special Committee.docx

I guess that would help, sorry about that.
J

From: Plater, Sharon MTIC:EX
Sent: Monday, April 18, 2016 12:36 PM
To: Biggs, Jackie FIN:EX
Subject: Re: FOIPPA Special Committee (2)
Hi Jackie. I have not received the document could you sen it to me.
Thanks

Sent from my iPhone

On Apr 18, 2016, at 12:03 PM, Biggs, Jackie FIN:EX <Jackie.Biggs@gov.bc.ca> wrote:

> Sorry....sent to wrong "S"....should have been Sharon originally.
> J
>
> **From:** Mitrou, Shirley MTIC:EX
> **Sent:** Monday, April 18, 2016 12:00 PM
> **To:** Biggs, Jackie FIN:EX; Plater, Sharon MTIC:EX
> **Subject:** RE: FOIPPA Special Committee (2)
> **Importance:** High
> Thanks for sending this Jackie, I don't know yet what changes David wants and whether its best for Sharon's area to make them – I'm fine with making changes but I also want to be efficient with our time as they have to be finalised today. Do you know what changes he wants? Is there a version that has his pencil edits etc?
> Shirley Mitrou
> *Ph:* 250 415-5402
>
> **From:** Biggs, Jackie FIN:EX
> **Sent:** Monday, April 18, 2016 11:42 AM
> **To:** Mitrou, Shirley MTIC:EX
> **Subject:** FOIPPA Special Committee (2)
> Hi Shirley,
> I understand that you have some updates to the attached note....sending the version from the main Finance site so you are working off a current copy.
> J

MINISTRY OF FINANCE
CORPORATE INFORMATION & RECORDS MANAGEMENT
ESTIMATES NOTE

ISSUE: Special Committee to Review the *Freedom of Information and Protection of Privacy Act* (FOIPPA)

s.13

CURRENT STATUS:

- The deadline for submissions to the Special Committee was January 29, 2016.
- Government did not provide a written submission to the Special Committee.
- Once completed, the Special Committee will prepare their report, including a list of recommendations which are expected to echo those of the Information and Privacy Commissioner. This has been typical of past Special Committees and is anticipated for this year as well.
- The Special Committee's final report is due by May 27, 2016.

KEY FACTS REGARDING THE ISSUE:

- On November 18th 2015, Government Chief Information Officer presented to the Special Committee on behalf of government. This presentation dealt largely with:
    - Data residency;
    - Harmonization with global privacy standards;
    - The increasing proliferation of records in a digital age;
    - Availability and impact of metadata;
    - Access through proactive disclosure;
    - Government's Privacy Management and Accountability Policy; and
    - Proposed housekeeping changes to FOIPPA.
- The Information and Privacy Commissioner also presented to the Special Committee and provided a written submission on November 18th.

s.13

s.13

- As part of the consultations conducted by the Special Committee, stakeholders from the public and private sector, as well as interested citizens, were also invited to present during four scheduled public hearings which took place in October and November 2015.
- Among the wide range of stakeholders who have participated in the public consultation, the Special Committee heard from the BC Freedom of Information and Privacy Association, the Centre for Law and Democracy, Vancouver Coastal Health Authority and members of the media.
- Though the Special Committee received presentations on a myriad of topics covering privacy, access, records management and government processes, the following issues were discussed in depth:
    - The inclusion of subsidiary corporations in FOIPPA;
    - Elimination of access fees;
    - Data residency;
    - The inclusion of a legislated duty to document key actions and decisions; and
    - Expansion of the "public interest" disclosure provision.
- Vancouver Coastal Health, on behalf of five other Health Authorities, made a submission to the Special Committee centered on desired changes to section 30.1 of FOIPPA. This section mandates that a public body must ensure that personal information in its custody or under its control is stored and accessed only in Canada, unless one of a small set of conditions is met.
- The Health Authorities have expressed discontent with this provision in the past. Among their many concerns, the health authorities have stated that, 30.1 impedes the flow of data, places unreasonable limitations on the use of cutting edge and cost-effective technology and inhibits remote access and technical support services.
- The Research Universities' Council of British Columbia has also provided a submission regarding section 30.1, noting concerns that this provision adversely impacts administrative efficiency, international engagement and student recruitment, online learning offerings and academic integrity.

From:	Sime, Mark MTIC:EX
To:	Edwardson, Jamie GCPE:EX
Cc:	Plater, Sharon MTIC:EX
Subject:	Government Presentation to FOIPPA Special Committee - Transcript
Date:	Friday, January 8, 2016 8:56:42 AM
Attachments:	image001.png Presentation Transcript - FOIPPA Special Committee.pdf

Good morning Jamie,
Sharon Plater has asked me to forward along the transcript of the presentation delivered to the FOIPPA Special Committee by CIO, Bette-Jo Hughes on November 18th. I have highlighted areas of the transcript where the s.13
s.13 . as I understand this is of particular interest. You will find these highlighted sections on pages 139-143.
Please let me know if you have any questions, or require anything further.

Mark Sime
Senior Legislative and Policy Advisor
Privacy and Legislation Branch
Office of the Government Chief Information Officer
PO Box 9412, Stn Prov Gov, Victoria BC V8W 9V1
Mark.Sime@gov.bc.ca
250 356-0388
cid:image001.png@01D00D5C.C083A670

LEGISLATIVE ASSEMBLY

PROVINCE OF BRITISH COLUMBIA

Fourth Session, 40th Parliament

REPORT OF PROCEEDINGS
(HANSARD)

SPECIAL COMMITTEE TO REVIEW THE

FREEDOM OF INFORMATION AND PROTECTION OF PRIVACY ACT

Victoria
Wednesday, November 18, 2015
Issue No. 7

DON McRAE, MLA, CHAIR

ISSN 1708-315X (Print)
ISSN 1708-3168 (Online)

SPECIAL COMMITTEE TO REVIEW THE FREEDOM OF INFORMATION AND PROTECTION OF PRIVACY ACT

Victoria
Wednesday, November 18, 2015

Chair:	Don McRae (Comox Valley BC Liberal)
Deputy Chair:	Doug Routley (Nanaimo–North Cowichan NDP)
Members:	Kathy Corrigan (Burnaby–Deer Lake NDP) David Eby (Vancouver–Point Grey NDP) Eric Foster (Vernon-Monashee BC Liberal) Sam Sullivan (Vancouver–False Creek BC Liberal) Jackie Tegart (Fraser-Nicola BC Liberal) John Yap (Richmond-Steveston BC Liberal)
Clerk:	Susan Sourial

CONTENTS

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

Wednesday, November 18, 2015

Page

MINUTES

SPECIAL COMMITTEE TO REVIEW THE FREEDOM OF INFORMATION AND PROTECTION OF PRIVACY ACT

Wednesday, November 18, 2015
8:30 a.m.
Douglas Fir Committee Room
Parliament Buildings, Victoria, B.C.

Present: Don McRae, MLA (Chair); Doug Routley, MLA (Deputy Chair); Kathy Corrigan, MLA; David Eby, MLA; Eric Foster, MLA; Sam Sullivan, MLA; Jackie Tegart, MLA

Unavoidably Absent: John Yap, MLA

1. The Chair called the Committee to order at 8:32 a.m.

2. Opening remarks by the Chair.

3. The following witnesses appeared before the Committee and answered questions regarding the *Freedom of Information and Protection of Privacy Act*:
1) Owen Munro, James Smith

4. The Committee recessed from 9:05 a.m. to 9:09 a.m.
3) Canadian Internet Policy & Public Interest Clinic (CIPPIC) Tamir Israel
4) Rob Wipond

5. The Committee recessed from 10:01 a.m. to 10:06 a.m.
5) Regional District of Central Kootenay Bronwen Bird

6. The Committee recessed from 10:26 a.m. to 10:30 a.m.

7. The following witnesses appeared before the Committee and answered questions regarding the *Freedom of Information and Protection of Privacy Act*:
Ministry of Technology, Innovation and Citizens' Services
- Bette-Jo Hughes, Government Chief Information Officer and Associate Deputy Minister
- Sharon Plater, Executive Director, Privacy and Legislation Branch
- Wes Boyd, Assistant Deputy Minister, Logistics and Business Services

Office of the Information and Privacy Commissioner for British Columbia
- Elizabeth Denham, Information and Privacy Commissioner
- Michael McEvoy, Deputy Commissioner

8. The Committee adjourned to the call of the Chair at 12:33 p.m.

Don McRae, MLA
Chair

Susan Sourial
Committee Clerk

WEDNESDAY, NOVEMBER 18, 2015

The committee met at 8:32 a.m.

[D. McRae in the chair.]

D. McRae (Chair): Good morning, everyone. My name is Don McRae. I am the member for Comox Valley and Chair of this committee, the Special Committee to Review the Freedom of Information and Protection of Privacy Act.

B.C.'s Freedom of Information and Protection of Privacy Act requires that a statutory review be conducted every six years by a special committee of the Legislative Assembly. This is the fourth such statutory review of FIPPA.

Our committee must submit a report to the Legislative Assembly by May 27, 2016, and may make recommendations to amend FIPPA. Our review is limited to scope. We are not mandated to implement our recommendations. Our committee would not be involved in any policy development or decision-making processes within government that might ensue in response to our recommendations. We are an advisory body only.

FIPPA is an access and privacy law that applies to the public sector. It gives access rights to British Columbians by requiring public bodies to disclose information in response to access requests and protects the privacy of individuals through limitations on how public bodies collect, use and disclose personal information. It also requires organizations to protect personal information by making reasonable security arrangements against the risks of a privacy breach.

At today's public hearing, we will hear from individuals and organizations as well as the Ministry of Technology, Innovation and Citizens' Services and the Information and Privacy Commissioner of British Columbia. Today's public hearing is the last one that's been scheduled, but written and audio and video submissions will be accepted by the committee until Friday, January 29, 2016. To make a submission — I would like to remind individuals watching at home — or to learn more about the work of the committee, visit our website, which is at www.leg.bc.ca/cmt/foi.

We have allocated 20 minutes for presentations, to be followed by an additional ten minutes for questions from panel members. The proceedings are to be recorded by our able Hansard people, and a transcript of the entire meeting will be made available on our website.

Just a full disclosure before we begin. I do not feel well today, and I will try not to pass my germs on to any of the committee members and definitely not to any of the people presenting.

I'll now ask the healthy Deputy Chair, to my left, to start by introducing himself, and we'll make sure the people at home know who's here.

D. Routley (Deputy Chair): My name is Doug Routley. I'm the MLA for Nanaimo–North Cowichan and Deputy Chair of this committee.

K. Corrigan: Kathy Corrigan, MLA for Burnaby–Deer Lake.

D. Eby: David Eby, MLA for Vancouver–Point Grey.

J. Tegart: Jackie Tegart, MLA for Fraser-Nicola.

E. Foster: Eric Foster, MLA, Vernon-Monashee.

S. Sullivan: Sam Sullivan, MLA, Vancouver–False Creek.

D. McRae (Chair): If possible, I'd like staff to introduce themselves as well.

S. Sourial (Committee Clerk): Susan Sourial, Committee Clerk.

H. Morrison: Helen Morrison, committee research analyst.

D. McRae (Chair): Thank you very much. Now, I believe we are doing our first video conference. Hopefully you can see us on TV. I think this is our first video presentation of the submission series.

[0835]

I believe I have Owen Munro and James Smith joining us from Vancouver. I'll turn the floor over to you.

Presentations

O. Munro: Great. My name is Owen Munro, and I'm with my colleague James Smith. We are journalism students at Langara College, and we are here today to present an argument about why student governments and student unions should be covered under the British Columbia Freedom of Information and Protection of Privacy Act.

We believe that student unions should fall under the same jurisdiction as public institutions, and we intend to show that the current system is both outdated and exploitative. It doesn't hold accountable student unions who collectively are in possession of millions of dollars across the country, and these student unions can sometimes overstep their roles within the B.C. Society Act to their own benefit.

FOI records are an essential tool for students and student journalists to hold university and college student unions to a high degree of accountability. Students are in a position where, despite having many available resources, they are placed at a disadvantage. Student unions are treated as a society in the B.C. Society Act and aren't transparent in their actions.

For students wanting to know more about their unions, from salaries to in-camera meetings to minutes, the most successful way of doing so is through the B.C. Society Act. Each student union is a registered society, but they are not recognized as governmental bodies, as some other functions would be, despite having many similarities to those governmental bodies.

They hold committee meetings and elections. They have control over student fees, which are mandatory. They use their own accounting systems, and they sign contracts with service providers, such as food and drink providers. They make decisions that really just affect student opinions and options as a whole, from clubs, activities, food and drink options and events. They are not unlike the structure we experience from any other governmental bodies.

We have very little influence on the interests of student unions that have become increasingly secretive and favourable towards their own benefits. In 2012, the Langara Students Union successfully eliminated their own members from attending in-camera meetings, a symbolic representation of their secretive operations toward the very people that fund them.

While we have the ability to request and to access information from our public institutions, the fact of the matter is that student governments are much more secretive, despite running essential services with fees that are mandatory of every student attending that public institution. Ironically, the fundamental service that a student union or government is mandated to provide is advocacy on behalf of the students.

There are many documented abuses of power by student unions and governments dating back to the inception of FOI laws in British Columbia. Section 19 of the B.C. College and Institute Act states that institutions must collect fees on behalf of student unions. This power is bestowed upon people who do not have the qualifications or meaningful experience to manage major sums of public money without being accountable to a certain standard of high quality.

There needs to be a level of transparency that ensures that our students' public money isn't being spent in unscrupulous ways and that we can trust our student governments are representing the best interests of students and not just their own agendas.

We would like to have something other to lean on than an exploitable B.C. Society Act. The society branch doesn't hold any power in regards to enforcement of the regulations to student unions. They can only remind student unions that the Society Act is in effect, but their power to do more so doesn't go beyond that.

For students to do anything beyond this, we must use section 85 of the B.C. Society Act and can request a superior court to remedy irregularities of student unions. This argument is underscored by the student unions' view, especially at Langara, that they cannot be challenged by students because they are aware of the time and the cost that it takes to find some form of justice for most students.

I can imagine the difference we would make if we were able to spot reckless and inefficient spending in our own student unions, not just at Langara, but other public institutions. That would be something that not just students but the general public needs to know.

There's no reason that we can't dismiss that culture of secretive behaviour, and there's no reason why we can't hold these student unions at the highest degree of accountability to ensure that every student receives the benefit of good, balanced governance.

[0840]

My colleague James Smith will now speak in-depth on specific occurrences that have happened at Langara and other public institutions in British Columbia in recent times. There have been many situations where the secrecy of our own unions have been in contravention of the B.C. Society Act and the principles which they claim to stand behind.

We have stood idly by for far too long without trying to make a profound impact on the systematic secrecy and unaccountability of the actions of student unions. There is vital information and data that is being withheld that urgently needs to be addressed for a transparent system that holds student unions responsible for their own individual actions.

I'll pass it over to James Smith now.

J. Smith: It's our position that student societies should be subject to the Freedom of Information and Protection of Privacy Act, as student societies are de facto part of the post-secondary institutions with which they're associated. B.C. post-secondary students collectively pay their unions millions of dollars every semester, yet there is little to no oversight to ensure that the money is spent responsibly or that the elected bodies adhere to their own bylaws or the statutes of the B.C. Society Act.

The union fees collected by the university, college or institution are mandatory, as is membership with the existing student society. It's mandatory and automatic. Anyone seeking a post-secondary education must, by default, join their institution's student society, making these societies as much a part of the school as anything else, such as classes or the school's administration.

A post-secondary institution, of course, has no say over how these student societies run, and rightly so. However, if a student — i.e., a union member — takes issue with how the union is being run, thinks the union is in violation of a bylaw, there's little recourse for them.

As members of a student society, we are guaranteed access under the Society Act to financial records, auditor reports, meeting minutes, etc. However, if we don't get access, or if the records are incomplete or unnecessarily censored, there's nothing we can do without hiring a lawyer, which we obviously can't afford to do.

While I can't speak directly to the situation at other post-secondary institutions, I can tell you that Langara Students Union, which controls the fees that are mandatorily collected by the college on their behalf, operates entirely behind closed doors and seems to do everything in its power to keep it that way.

I know that journalist and Langara alumnus Stanley Tromp mentioned the LSU briefly in his presentation before this committee on Monday, November 9. As student journalists, it is our duty to keep the public informed about the issues that affect them — in this case, how millions of dollars of their money is being spent by a group of inexperienced people with little to no oversight.

Every year, the LSU council designates a new elected member to act as their immediate liaison. That person is our sole point of contact. All other elected members and paid staff are barred from talking to us under any circumstances, citing LSU policies that aren't available on their website or anywhere else and that they won't show us a written copy of. The media liaison, regardless of who it is, is often hard to reach and, as often as not, leaves us without comment before deadline.

Efforts to get the information we want ourselves are equally frustrating. The LSU bylaws require all members, not just those in the media, to give 48 hours notice to inspect any and all documents to which we're legally entitled. The bylaws do not specify any specific officer or adviser or staff member or councillor who must be present to release these documents.

This fall, the LSU cancelled their annual elections two days into their four-day polling. When we asked why, we were refused comment. Eventually a brief release was posted on the LSU website, saying that the elections had been cancelled due to "numerous irregularities." No further explanation has been given. When the LSU finally announced new elections two weeks ago, all the previous candidates were still on the ballot, leading to renewed questions about what exactly had prompted them to cancel the original elections. But once again, no explanation has been given, nor, at this point, frankly, do we expect that there will be.

[0845]

When one of our reporters went down to the LSU office to look over their budget information to determine how much the cancelled election had cost, he was told that they couldn't release those documents to him, despite acknowledging they'd received his request over 48 hours before. When the reporter asked why, they said that they couldn't share those documents without the financial officer present. I remind you that there is no language in the LSU bylaws saying that any specific person is needed to release documents to members.

I myself encountered a similar situation two weeks ago. I submitted my request to view financial documents and meeting minutes to the LSU and was told they would let me know when the documents were ready. I waited a week and a half without hearing from them and eventually went down to see if they were ready.

The budget and auditor's reports that I asked for were there, but only because they had been lumped in with another reporter's request. The regular meeting minutes, the annual general meeting minutes and list of elected members and paid staff, all documents that should by rights be readily available and public, were not there. When I asked for the rest of the documents and handed them a printed copy of my request, I was told that they had never received it. However, this isn't possible, as the other reporter hadn't asked for the auditor's reports, essentially proving that they had in fact received my request.

In the end, I was told that they needed more time to find the documents I'd requested, and I'm still waiting to hear whether they've located anything.

In the interests of full disclosure, the bylaw pertaining to inspection of records at the LSU, article XIII, doesn't give any timeline for compliance with requests by members, not even the traditionally ambiguous reference to "a timely manner."

Of course, when we do get to see the documents we request, it doesn't necessarily do us any good. LSU bylaws require that anyone inspecting any documents be supervised by staff or an elected member, even when inspecting something as seemingly benign as regular council meeting minutes, "to ensure" — I quote directly from LSU bylaw article XIII — "that records are not reproduced or noted in any way."

This policy not only makes it very difficult, if not impossible, to ensure accuracy or any kind of in-depth analysis in our reporting; it also makes it virtually impossible for any member to analyze and understand how the millions of dollars of students' money is being spent.

Adding to the culture of secrecy at the LSU, all meetings are conducted behind closed doors. The public and membership are not allowed to attend these meetings, as per article 5.14, called "Closed council meetings," of the LSU bylaws.

In addition, an unknown number of meetings are conducted in camera and off the books, making it impossible to fully know what the union is doing or how decisions about the spending of students' money are being made.

As required by the Society Act and its own bylaws, the LSU does hold annual general meetings. However, for the last three years these have been held in late June or July, always in the middle of the day and midweek when the majority of the public who fund the LSU throughout the year are not present and are often not even enrolled. This past summer, enrolment at Langara was little over half what it is this fall, just to give a bit of context.

The timing of the meeting, when, as I said, enrolment is half what it is during the fall or spring and at a time when most people are at work, appears to be a further effort to limit the members' access to those in power at the LSU.

It's also worth noting that the LSU council only sits between September and April, according to their own bylaws. They aren't even in session when the AGM happens.

The extreme level of secrecy at the LSU allows them to operate however they want and do whatever they want with few to no checks and balances. The lack of oversight for the LSU and other student societies in our province has led to many instances of malfeasance over the years, from election irregularities to mismanaged funds and, in at least one recent extreme case, alleged embezzlement.

Between 2005 and 2011 the Kwantlen Student Association was embroiled in a series of scandals connected to their one-time director of finance and chairperson of the board, Aaron Takhar, and the Reduce All Fees slate of candidates, including mismanaged and missing funds, election improprieties and more lawsuits than I can count.

[0850]

PricewaterhouseCoopers was commissioned in 2006 to do a forensic audit of the association. That audit found nearly $150,000 of student funds had been spent without supporting documents, including $67,000 paid to Takhar's consulting firm, AST Ventures. AST are Takhar's initials. The society had also given out $620,000 in high-risk and unsecured loans, plus a $200,000 loan from a fund that was designated strictly for KSA health and dental expenses.

Despite the KSA launching a lawsuit against Takhar, the allegations in the audit were never proven in court. It's because relatives of Takhar's were later elected to the executive board of the KSA. One of them was designated the board's sole contact with the legal team and subsequently instructed them, with the support of the board, to drop the suit.

To the best of my knowledge, none of that money was ever recovered. That's not even the entirety of the KSA saga. A quick Google search can fill you in on all the other details.

Of course, issues involving student societies are not always, or even often, because of malicious intent by its elected members. These are young people with little to no experience in politics, finance, law or leadership. Many, if not most, of them are often in it for a bump to their resumés. For example, a student at Langara who wants to transfer to UBC has to have extracurricular activities, like student government, on his or her resumé in order to get accepted. He or she may have no interest in it otherwise.

Turnover in these organizations is also a factor. In general, students are only in post-secondary for two to four years. While again, I can't speak to the bylaws and practices at other student societies, under the LSU's current bylaws, elected members aren't allowed to hold the same position for more than one term — i.e., year — and may not serve more than two terms total during their time at college, virtually guaranteeing a perpetually inexperienced council.

It is our position that if student societies were subject to FOIPP Act, they could better be held accountable to their public membership, which mandatorily pays its fees through public institutions. FOIPPA requests can be costly, but they're far cheaper than court cases and more readily available for the public to use — especially students.

Though it would do nothing to force the LSU's media liaison to talk to our reporters more or things like that, it would give us one more tool in our tool belt by which to hold them accountable. Perhaps by ensuring a little transparency, they'll be better able to serve their constituents.

D. McRae (Chair): Thank you very much, James. You and Owen took up about 18 minutes, which allows us 12 minutes for questions if committee members have such.

K. Corrigan: Thank you, Owen and James. I'm Kathy Corrigan, MLA for Burnaby–Deer Lake, but I'm also the Official Opposition spokesperson for Advanced Education. Not only because of the content as it relates to what we're doing on this committee; I'm also interested because of my role as spokesperson.

I'm wondering. We've had submissions suggesting that subsidiaries at post-secondary institutions or other government bodies should be FOIable. Are there other, comparable types of organizations? I'm thinking of the Legal Services Society, which is another society, which is FOIable.

But student unions' funding comes entirely — or, I would assume, almost entirely — not from government, but from the students themselves. I'm wondering if you see that as a distinction or a reason why we couldn't include student unions. Have you done any looking at trying to get comparables to what you're suggesting?

O. Munro: I think, mostly, if students specifically are paying these mandatory fees, we haven't exactly looked into any sort of comparables. But what we have looked into is how these student fees relate to what they get in terms of funding, and that being FOIable, at least to ensure some sort of transparency and accountability for how they end up spending those fees.

[0855]

But no, we haven't looked at many other comparables, such as the legal society that you brought up.

K. Corrigan: Great, thank you.

D. Eby: I very much appreciate your presentation. I'm very concerned about the information you presented about what's happening at Langara, as an advocate for open government and transparency at all levels.

One of the challenges I have, though, is the old adage: "Hard cases make bad law." If all the allegations that you're making are true, designing the Freedom of Information

Act to respond to a serious issue at a single college…. Not to say that there haven't been issues at other student unions, but there haven't been other student unions that…. I was reading about the 2012 referendum, for example, where students at Langara apparently voted in favour of restricting their own access to meeting minutes and these kinds of things — a very unusual situation.

Can you tell me about how unique these issues are to Langara and why it would be that students would actually vote in favour of restricting their own access to information from their student government instead of voting for what you're suggesting, which was expanding public access to those documents?

J. Smith: That was before either of us were at Langara, so I can't necessarily speak directly to it. I can say, from my off-the-record conversations with LSU staff…. They explained that their concerns were a combination of worries about being misquoted. We're student journalists, and they're students as well. Obviously, both parties are trying to learn how to negotiate the situation and how to best do their job.

Student journalists make mistakes. Those mistakes and alleged misquotes were part of the reason why the LSU did not want student journalists or students in general at the meetings. Another reason is because, basically, it made them uncomfortable. It made them worry that they couldn't openly discuss things and couldn't…. They were too worried about making a mistake, publicly, to effectively discuss and make decisions.

D. Eby: I definitely understand why the student government would be in favour of amendments that would restrict public access and help them control messaging. We've seen that inclination in various levels of government that restrict transparency and restrict access to documents. What I don't understand is…. It looks like there was a referendum in 2012 — unfortunately, you can't speak to that — where the students, as a whole, at Langara…. Admittedly, there was low voter turnout, but they voted in favour of restricting access.

It seems like there's been a bit of a shift, if what you're telling the committee is accurate. So if I could just get you to comment on how unique the situation is at Langara — whether the change made by this committee would put undue bureaucratic obligations on to a number of small committees with, admittedly, large amounts of money at the university level but limited resources to fulfil freedom-of-information requests and whether we do that for the entire province to respond to a single situation at Langara.

O. Munro: If I can take this one. This isn't necessarily a situation that is unique to Langara. This is a situation where many other student unions — whether it be Kwantlen, UBC, Douglas College…. This is happening all over, not just Langara. So if we could have some sort of FOIable system where we can at least see the minutes that these meetings have produced, even if it wasn't an in-camera meeting, and have some sort of accountability that way….

These are elected members that we students have elected to represent us. They represent the interests and needs of every student. It's definitely not a situation that is unique to Langara.

[0900]

J. Smith: Using the example of the Kwantlen Student Association and that whole situation, the executive board members and that were a group of friends and relatives of Takhar. Even when the meeting minutes and that kind of thing are publicly available, as they are with some student associations…. They do put their minutes and financial records and that on line and openly available in their offices. That doesn't necessarily let us know how a group of students, like in the KSA example — which, admittedly, is an extreme example — would coordinate their efforts outside of the meetings.

FOI access to things like e-mail records and that would help uncover things like that kind of alleged corruption and collusion in order to maybe stop the problem before it gets out of hand.

D. McRae (Chair): Kathy, I believe, has one more question.

K. Corrigan: It's similar to my earlier question. And I would like to echo what Mr. Eby said. I really do appreciate your presentation and the work that you do.

What I'm wrestling with is what we define as government. I think that FOI legislation is meant to cover government and government bodies. What I'm trying to figure out is: is a student union a government body? Maybe it can be extended to bodies that are funded by government bodies or to programs that are done for the purposes of providing public services.

I'm wrestling a bit with that concept of whether or not a student union is a government-related body. I'm wondering if you've got any comments on that.

J. Smith: I believe that the student unions are different from other societies, such as trade unions, in that there's no option about membership. In your career, you can choose to join a union workplace or a non-union workplace. Depending on your career, that choice can be very limited, but it is there. If you want a post-secondary education, which you have to have these days, you have to join these unions. You're not really given a choice in the matter. As I said, it's mandatory, and it's automatic.

For us, that makes a student union a de facto part of the post-secondary institution, even though the post-secondary institution doesn't have any say over how not

just the LSU but the student societies run. In that way, I think it's different. It's kind of a unique situation compared to other societies covered by the Society Act or the FOI people.

O. Munro: I think, as well, there's…. You look at some of the functions that LSU and all student unions have. They have elections, and that's one of the major fundamentals, I believe, of having a governmental body. I kind of equate it to, if we can imagine, some other form of government holding an election and then closing it because of numerous irregularities and not giving the people that they represent a chance to have their voice heard. I feel like that is very much functioning like a governmental body.

They make decisions that are based on behalf of students. They advocate for students. But again, I go back to the election thing as something that's very much like a governmental body. I think, in that context, they should be regarded as a governmental body.

J. Smith: Also, the money the LSU manages is coming from students. A good chunk of that money is coming from the government through student loans and student grants as well. And the LSU…. Sorry, I keep saying the LSU, and I mean to be more general. The student unions advocate for students and have, often, a seat on the college or university board, which puts them essentially as an elected member on the governing body of a public body.

Again, that lends itself to my argument that they are a de facto part of that public body.

D. McRae (Chair): Perfect. Thank you very much.

It is 9:05. I'm going to ask the committee for a very short recess while we connect with our next presenter via teleconference. We'll resume in a couple of minutes.

Thank you very much, Langara.

The committee recessed from 9:05 a.m. to 9:09 a.m.

[D. McRae in the chair.]

D. McRae (Chair): We're going to resume the committee deliberations. We are joined via teleconference by Tamir Israel, joining us from Ottawa.

Tamir, you are being joined with five committee members right now. By practice of the committee, we would ask that you do a presentation of approximately 20 minutes — less if you need to. Then I will allow the committee members ten minutes to have a question-and-answer period with you as well. Are you okay with that?

[0910]

T. Israel: Yes, that's great. Thank you.

D. McRae (Chair): Perfect. Tamir, it is now, according to my watch, 9:10. I will turn the floor over to you, sir.

T. Israel: Thank you. Good morning, Mr. Chairman and members of the committee. As the Chairman mentioned, my name is Tamir Israel, and I'm staff lawyer with CIPPIC, the Canadian Internet Policy and Public Interest Clinic, at the University of Ottawa's faculty of law. I'm also a member in good standing of the Law Society of Upper Canada. CIPPIC is grateful for the opportunity to provide our input into this committee's review of the B.C. Freedom of Information and Protection of Privacy Act.

CIPPIC is a law and technology clinic that works to advance the public interest in policy debates at the intersection of law and technology, which is our core mandate. We additionally provide pro bono legal assistance to under-represented organizations and individuals on law and technology issues and provide legal and public education on related matters.

CIPPIC's expertise in this field has evolved through its myriad public advocacy activities on this front, which include interventions at various levels of court, involvement in Internet governance–related matters before various quasi-judicial tribunals and international fora, the publication of academic and research reports on Internet-related issues and expert testimony before parliamentary committees such as this one.

While CIPPIC has wide-ranging interests in issues related to privacy, data protection and freedom of information, I have been asked today to provide an overview of potential implications arising from trade agreements for B.C. FIPPA's data localization mechanism encoded in section 30.1.

My comments today will therefore present a change of pace from testimony heard so far by this committee, as I'll be restricted to that topic. We do, however, reserve the option of providing a more comprehensive written submission within your comment period, and I will also make available to you my oral comments today in writing, with some annotations and references, in case you want to read further.

In my comments today, I'll first provide an overview of section 30.1 in the foreign intelligence context, followed by an overview of recent developments in trade agreements, and then I will close with some details on specific or potential implications of trade agreements for section 30.1 of B.C. FIPPA.

At the outset, I'll address section 30.1 by way of background. However, the core of my submission will relate to the trade implications. As the committee is aware, section 30.1 was enacted out of concern that outsourcing of storage of Canadian data, and particularly of health information, to the United States would subject this data to an excessive investigative context that places few limits on state data-gathering activities.

The passing of the U.S.A. Patriot Act was, at the time, pointed to as an example of the expansive powers granted to the United States agencies. However, a less notorious yet far more serious United States law, the FISA Amendments Act of 2008, is the true source of concern for Canadian data. It provides United States intelligence agencies — primarily, the National Security Agency — near limitless powers to access information of foreigners.

While these powers are so broad they incidentally capture significant amounts of U.S. data, they at least provide some minimal protection for non-foreigners, in the nature of restrictions on use, further disclosure and identity suppression. These protections are not available for data of foreigners.

The NSA has not hesitated to make full use of its expansive powers, and documents released by former NSA contractor Edward Snowden demonstrate that the agency obtains an average of 100 million pieces of data from United States–based computer networks on an average day.

A detailed qualitative analysis of NSA's stored data obtained by the *Washington Post* demonstrates the expansive nature of the resulting data collection programs. This analysis found that only 10 percent of the 11,000 individuals whose data was present in the sample were actual NSA targets, the rest being individuals whose data was collaterally captured in getting to those 10 percent.

Given the minimal technical and legal constraints on the NSA, no effort is made to discard files openly acknowledged by the NSA itself to be irrelevant. Regarding the quality of this collateral impact, the *Washington Post* describes it as such: "Many other files, described as useless by the analysts but nonetheless retained, have a startlingly intimate, even voyeuristic, quality. They tell stories of love and heartbreak, illicit sexual liaisons, mental health crises, political and religious conversions, financial anxieties and disappointed hopes." The individual profiles themselves specifically included medical records, resumés, children's academic transcripts and sensitive pictures, described by the *Washington Post* as risqué. [0915]

The foreign intelligence framework put in place by the FISA Amendments Act of 2008, which grants the NSA carte blanche regarding the privacy of foreigners, is starkly at odds with the interconnected nature of our modern global digital activity.

Canada, it should be noted, is not immune from this paradigm, as our own foreign intelligence agency, the Communications Security Establishment, or CSE, is granted similar leeway when gathering information of non-Canadians, as are other foreign intelligence agencies around the world. Collectively, this entire paradigm creates significant cross-border challenges for those governments hoping to provide some measure of privacy for their citizens while still finding ways to participate in the global communications infrastructure.

Data localization restrictions, such as that encoded in B.C. FIPPA's section 1, 30.1, Nova Scotia's Personal Information International Disclosure Protection Act and Australia's Personally Controlled Electronic Health Records Act, provide examples of these attempts.

Territorial restrictions of this nature are not a silver bullet, however. They fail to directly address the underlying problem, which is the disregard for privacy of foreigners that is at the heart of many foreign intelligence frameworks. Even with data localization measures, foreign intelligence agencies can — and regularly do — reach into foreign territories and compromise data centres remotely.

Gaining this type of remote access requires greater practical effort, has accompanying exposure risks and lacks the ease associated with compelling a domestically present company to merely comply with access orders. Nonetheless, remote access is pervasively employed by foreign intelligence agencies. Moreover, these agencies situate themselves at key points in the global communications infrastructure and capture significant amounts of data in transit.

On the other hand, territorial restrictions can lead to greater privacy by increasing the difficulty by which foreign intelligence agencies can gain access to such data. Moreover, they can lead to the adoption of stronger privacy protections more generally. For example, concern over foreign intelligence agencies, such as the NSA, has pushed companies such as Microsoft to develop clouds based in local data centres in several jurisdictions, including Canada, India, Germany and Ireland, as well as to seek legal recognition of this data segmentation scheme in U.S. courts.

It has also provided the B.C. government, as you are likely aware, with the incentive and impetus to negotiate enhanced protection, such as tokenization schemes, with a foreign-based cloud computing company and services.

Notably, it has provided the basis for negotiations between the European Union and the United States, with the object of securing better protection for EU citizens within the United States foreign intelligence framework. These negotiations arose in response to a decision of the Court of Justice of the European Union invalidating the ability of private companies to transfer data to the United States because such companies cannot provide protection against the NSA's excessive foreign intelligence regime. These bilateral EU-U.S. negotiations regarding the need to adopt protections for EU citizen data within the United States foreign intelligence regime only arose out of the EU's data transfer restrictions.

With this general discussion of the potential and limits of data localization as a means of safeguarding domestic data against foreign state agencies in mind, I now turn to a discussion of recent developments in trade frameworks and their potential implications for this specific data localization regime.

Some general background on trade agreements. While earlier ways of trade agreements have had as their primary object the reduction of tariffs as a means of trade liberalization, more recent trade initiatives have begun to address significant elements of domestic regulation in an attempt to harmonize and set specific standards.

The result of this shift is that impact of trade agreements is no longer primarily economic in nature, and the potential of such agreements to undermine the ability of states to protect their citizens is high.

The trend in question has taken hold in earnest with respect to domestic intellectual property laws and is beginning to encompass a growing range of the digital ecosystem that primarily falls to provincial control under Canada's constitutional scheme. This includes privacy protection, e-commerce, transactional protections and neutrality obligations.

The trend poses significant issues for democratic legitimacy, as the autonomy granted, to the executive branch of the federal government in particular, to enter into foreign policy commitments in secret and without meaningful consultation with the public is broad.

[0920]

Where this autonomy was historically limited to negotiating trade quotas and tariffs by practice, the impact of these processes on domestic regulatory policy was more limited. However, trade agreements today include significant and detailed obligations regarding domestic regulatory regimes, and this trend is only likely to intensify in the future, meaning that the impact on domestic regulatory regimes, such as B.C. FIPPA, is likely to be an ongoing process.

The shortcomings of the trade process as an instrument of legitimate democratic policy-making are significant. The instruments are negotiated in highly secretive contexts with substantive texts outside the reach of not only the public and of freedom-of-information laws but even of parliamentarians. This creates difficulties in attempts to ensure that the policy outcomes, which are ultimately encoded in trade agreements, reflect the public interests, as the public is effectively locked out of the policy development stage.

I take an aside to note that this is not necessarily something that is within your purview to address, but it does form the basic backdrop of the agreements that you are dealing with, will have to deal with, now as well as in the future.

Once a trade agreement is completed, it is presented to the public as a fait accompli. Increasingly, the obligations undertaken in trade agreements are detailed and specific, allowing for minimal latitude in how these are ultimately encoded in domestic legislation or action. This leaves any ex post democratic protections an inadequate safeguard for ensuring balanced public policy.

Even without legislative action, trade commitments can have direct impact on domestic policy and law. Our courts will interpret, for example, ambiguities in domestic legislation in a manner that presumes compliance with international commitments such as trade agreements. Even where commitments undertaken in a trade agreement do not make their way into domestic legislation or judicial decisions directly, the ability to enforce trade commitments can impose heavy consequences for domestic governments operating regulatory regimes that do not comply with these.

There are, in essence, two types of enforcement mechanisms that have taken root in trade agreements in recent years. I'll just explain them briefly.

The first and more insidious of the two is the inclusion of investor-state dispute resolutions, commonly referred to as ISDS, rights that grant foreign investors the right to sue domestic governments in international tribunals as a means of challenging regulatory actions of those governments. This is a powerful instrument placed in the hands of one set of stakeholders, foreign investors, while ignoring all others.

A second only somewhat less concerning means of enforcing trade obligations is through the inclusion of bilateral dispute resolution measures, referred to commonly as simply dispute resolution, which allow one state government to sue another over perceived violations of rights. The ambiguous nature of trade language has meant that these dispute resolution mechanisms can sometimes lead to surprising and unpredictable outcomes.

For example, in 2005, a World Trade Organization appellate body upheld an Antigua and Barbuda lawsuit that emerged from a series of United States laws designed to prevent on-line gambling. This lawsuit succeeded, even though the United States had not intended to make any trade commitments relating to the regulation of gambling at all. The remedy granted to Antigua was the right to violate U.S. intellectual property laws in order to recover its annual losses, estimated at $21 million a year, until the United States Legislature took steps to address the repudiated gambling regulation.

Dispute resolution mechanisms can even be used by foreign governments or investors, as the case may be, to challenge the results of domestic judicial decisions interpreting laws previously thought to be compliant with trade obligations in a manner that negatively impacts the party in question.

For example, pharmaceutical company Eli Lilly recently filed a $500 million lawsuit, under NAFTA's investor-state dispute settlement regime, against the federal Canadian government. The lawsuit arose out of a Supreme Court of Canada decision that evolved patent obligations in a manner designed to prevent patent holders from claiming patent protection over outcomes that are never realized.

It is notable that the public interest is not only locked out of the trade commitment development process but also locked out of the ex post judicial development of

these commitments. In democracies, lawsuits, class actions and constitutional challenges can be launched by individuals and companies alike. Under the trade regime, however, it is only companies or states that can initiate such processes.

[0925]

Moreover, whereas in most democracies, constitutional restraints exist as an ultimate limit on the impact of regulator action, the highest consideration in the application of trade commitments becomes the overriding need to limit barriers to trade.

Currently this creates an atmosphere where it is difficult for any gold standard to emerge or prevail. There have already been documented instances in Canada, for example, where the spectre of trade enforcement was used to chill certain public policy initiatives that would have set higher protection standards — primarily in the environmental protection context.

In this regard, Eli Lilly's stated justification for challenging Canadian patent law under NAFTA is telling. The quote here from the Eli Lilly representative is that they didn't like the result of the Supreme Court decision, but they also say: "We're afraid it can lead to other countries attempting to undermine intellectual property in similar ways."

The decision was held by other commentators to be very reasonable and a positive advancement of intellectual property laws and patent laws.

In addition, a country that first adopts a higher standard may have a harder time justifying the standard in question in the manner required by many trade agreement prohibitions.

Now, all of this is by way of background, but it does have specific implications for any potential defence of section 30.1. So against this backdrop, data localization rules, such as those of British Columbia, Nova Scotia, Australia and India, have all been explicitly and increasingly targeted, primarily by United States–based information technology industry groups and, as a result, by the United States trade representative.

This has made data localization a live issue in three major regional agreements, which include the recently concluded Trans-Pacific Partnership agreement, referred to as the TPP; its east coast counterpart, the Transatlantic Trade and Investment Partnership, the TTIP; and the global Trade in Services Agreement, referred to as TISA.

Each of these agreements includes similar sets of commitments, modified for the particular regional context and negotiated outcomes that limit data localization requirements. The commitments adopted in these agreements are co-extensive, meaning that Canada will be subject to all of these, in addition to its existing commitments under NAFTA, GATT and GATS.

The most salient features of these new agreements is the electronic commerce chapter. This chapter directly addresses privacy generally as well as data localization laws specifically. The Trans-Pacific Partnership agreement's — from now on in my comments, I'll refer to it as TPP — e-commerce chapter includes explicit data localization restrictions, as does a leaked draft of the Trade in Services Agreement, which is still being negotiated.

While the TPP e-commerce chapter was initially reported as imposing limitations on private and public sectors alike, the final version, as adopted, excludes government procurement and government data collection from its scope. This effectively immunizes B.C. FIPPA's section 30.1. However, the finalized TPP provision is nonetheless instructive, as it may be applied to state action in future agreements.

The provision adopts a general prohibition on state attempts to prevent cross-border transfer of information as well as from requiring the local presence of computing facilities. States can depart from these prohibitions but only if a rigid justification test is met. This test includes a need to prove that the restriction in question does not extend further than strictly necessary to achieve a legitimate public policy objective.

In the context of section of 30.1, if the public policy objective is established to be placing barriers on the ability of foreign intelligence agencies to access personal information of Canadians, then the onus will be on the government to demonstrate that the provision does, in fact, achieve its objective.

The data localization restrictions in TISA's, which is the still-being-negotiated counterpart to the TPP, most recently leaked e-commerce chapter are even more restrictive. To begin with, they apply to private and public sector action alike. Moreover, they adopt a categorical prohibition to data localization that brooks no limitation. This may change over time as the text gets negotiated.

[0930]

Both TISA's and TPP's e-commerce chapters are subject to enforcement through state-to-state dispute resolution. The TPP also includes an investor-state dispute resolution chapter, which, in its final iteration, does not apply to the rights granted in its e-commerce chapter.

As a result, even if TPP's explicit data localization obligations were applied to the public sector, the Canadian government would not be subject to direct company-initiated lawsuits over section 30.1 arising from the e-commerce chapter. However, the TPP's investor-state dispute settlement regime does grant foreign investors the right to sue governments over any treatment of domestic companies or companies of another country that is more favourable in like circumstances than that according to its own company.

I know I'm near the end. Can I just take another half a minute?

D. McRae (Chair): You can have 30 seconds. It will take away from our question-and-answer period, but 30 seconds is yours.

T. Israel: I'll finish it really quickly. The viability of section 30.1, under this regime, will largely turn on what is considered like treatment. This will turn on the government's ability to demonstrate that the distinction drawn by the provision between Canadian-based and foreign data storage is based on real differences between the two.

I'll just say very briefly that there has been one trade decision that has acknowledged that data localization can be justified under these more generalized types of obligations. However, it requires a very detailed explanation of why specific countries or the countries that are being restricted from providing the storage in question need to specifically be excluded from the procurement in question.

I'll just finish off there. Thank you for the additional time.

D. McRae (Chair): Well, thank you very much. I know I have two questions.

D. Routley (Deputy Chair): Two things, Mr. Israel. Thank you very much for your presentation. It was very helpful.

The first would be…. We heard, at a recent conference, from Lisa Austin from the University of Toronto, who pointed out that should B.C.'s personal information be stored in the United States, we, of course, are not protected by Fourth Amendment rights as non-resident foreigners.

She also indicated that we would surrender our Canadian Charter rights, because any search of that information from across border — the agency making that search — would not be required to respect our Charter rights. That would be the first question. Do you agree that that would be a consequence of storing information in the U.S.?

Then secondly, provinces have made different reservations under TPP. Alberta has reserved their Legislative Assembly as well as all officers of the Legislative Assembly, and Nova Scotia has reserved their chief information officer as well as their health chief information officer, whereas B.C. has only reserved the Legislative Assembly. Could you share with us what you think the implications of those reservation choices are?

T. Israel: Sure. To the first issue, the foreign intelligence paradigm that, particularly, the NSA but also other agencies operate under has as its underlying presumption the mistaken, in my view and increasingly in the view of international law, but strongly held assumption that privacy essentially ends at your territorial borders. Again, this is not limited to the U.S. Canada applies the same standard to non-Canadians.

The result of this is the unfortunate reality that yes, a Canadian whose data is being accessed by an agency in the U.S. and who is not in the U.S. at the time, even though their data is, cannot assert any constitutional privacy right at all, which is a real gap when you consider how globally integrated our communications are. So the answer to the first question is yes. The moment the data is being accessed from the United States through the aegis of a U.S. company who has control over that data, there is no privacy right that the Canadian affected can really assert.

[0935]

Now, this does apply, as well, if the U.S. agency hacks into, say, a Canadian-based data centre holding the same data. Arguably, though, there are other issues there that could violate Canadian criminal law, for example, or other types of laws in Canada that could, in theory, be raised against the agency in a way that couldn't happen, necessarily, if the data was only stored in the U.S. I hope that answers question 1.

To question 2….

D. Routley (Deputy Chair): Just before you go there, could international treaty-making that would extend a person's citizenship rights along with their data across borders — is that a reasonable solution under agreements that we now are subject to?

T. Israel: The problem there is the international human rights instruments, which are universally the broadest adopted and ratified instruments on the planet, do not have the powerful enforcement mechanisms that come in the trade context. So my argument would….

The U.N. High Commissioner for Human Rights has said that privacy should be treated as applying extraterritorially and should be respected even with respect to foreigners, but governments like the United States — and Canada, in its own practices — do not accede to that, and there's no way to compel them to by going to an international tribunal in the way that an obligation in a trade agreement can be enforced.

So the answer is yes and no. Yes, technically, but there's no way to impose that practice onto U.S. agencies. What's happening now between the E.U. and the U.S. as a result of the…. Data has been cut off from flowing to the United States, but the Court of Justice in the European Union has said that there are not sufficient guarantees for European citizens' data. So now this forces the United States to negotiate with the U.S.-specific protections for European citizens' data.

There's no other…. It's very difficult to get there from a practical perspective. It's really the challenge on that. Data localization limits are one of the few ways that you can negotiate those types of protections, just as they are a key impetus for negotiating additional privacy protections, such as tokenization with specific service providers.

Very quickly, to the second question. Yes, reservations can play a role. Under TPP and with the specific context of the e-commerce chapter…. I think the answer

is: definitely it would have been, probably, better to get a broader set of reservations that would have provided more latitude for this type of activity, for the B.C. government more broadly. But as it stands, the reservations won't help under TPP. They may under future agreements, if that is undertaken.

D. McRae (Chair): Thank you very much. In the reflection of brevity, we are down to about two minutes. So I wonder, Kathy, if you could ask a quick question, and hopefully Tamir could answer a quick answer. We'll see if we have time to squeeze in David Eby's question at the end.

K. Corrigan: Thank you very much. I share your concern about the impact of trade agreements, particularly on subnational governments that have not been involved in negotiating those trade agreements and yet are subject to them as well.

I just wanted to clarify, though. You were saying that the TPP has excluded government. So that would reflect the safety of 30.1 as far as we're concerned. You're talking about like treatment. But as long as we have the exclusion, then we are not being subjected to the like treatment. It's simply an excluded area, so we're, so far, protected. Is that correct?

T. Israel: Yes. Sorry, I think I rushed through the end there. There is an explicit prohibition on data localization that does not apply, but there is a more general like-treatment requirement of general application that could apply. It's not designed for this type of thing, but it could apply.

It's hard to predict what a trade tribunal will do, unfortunately. But creating a more concrete record for why the restriction is there is a prophylactic against that type of thing.

D. McRae (Chair): We have time for a quick question and a quick answer, from David Eby.

D. Eby: Maybe just a request that Mr. Israel…. I have a lot of questions but, unfortunately, no time. I would hope that you would follow this up with a written submission with specific recommendations for this committee in relation to our job here, which is to make recommendations related to the amendment of B.C.'s Freedom of Information and Protection of Privacy Act.

[0940]

A lot of interesting international trade questions you've raised. Very difficult for this committee to incorporate amendments to TPP or other international trade agreements. So specific to B.C., if you have a list of recommendations for this committee, I'd love to hear them, because I share your concerns. I'm just not sure of the extent of our committee's work at that level.

T. Israel: If I could respond really briefly, I think I wanted to provide some assurance that you're probably under no immediate trade obligation to change section 30.1. We will try to provide more detailed comments on that as well as on some other elements of the law, as it is something that we're interested in.

D. McRae (Chair): Tamir, thank you very much for your presentation. Adding to what David Eby was just saying, we can take a written submission up to January 29, 2016. Thank you very much for your oral presentation, and if you wish to submit one in writing, it would be much appreciated by committee members. Thank you for joining us today.

T. Israel: Thanks for having me.

D. McRae (Chair): I would ask Rob Wipond to come join us, please.

Rob, I know you've been here for the last several presentations. We try to keep the actual oral presentation to 20 minutes and then ten minutes for questions and answers. Since you're actually here in person, I will maybe give you a hand signal if you get close to your 20 minutes and you're going strong. I just open the floor to you.

R. Wipond: Yes, I'm going to monitor my time here, too, and maybe just cut some things out if I feel like I'm going a little too quickly.

Good morning. I'm a freelance investigative journalist based in Victoria, and I've been using information access law for two decades. One of the topic areas that I research and write about is surveillance and privacy. I'm going to review some examples that show why we need more information access and privacy monitoring, enforcement and penalties, and then I'm going to focus on a very specific recommendation for an addition to schedule 2 of FIPPA.

Laws covering information and privacy have become some of the most important laws of our time. Issues of surveillance, privacy and citizens' rights to know what their governments are doing are central to democracy. The role you are playing right now in reviewing FIPPA is arguably one of the most important tasks facing our government.

FIPPA is valuable legislation. It has, unfortunately, been steadily weakened while it desperately needs to be strengthened. For example, the government received excellent feedback from a public committee that it organized to provide input about the B.C. Services Card. Their report is valuable reading, and I found it inspiring to see how much a diverse group of ordinary citizens, through the process, came to truly understand and care about protecting privacy and about the dangers of surveillance.

As far as I have seen, the government has, by and large, ignored their input and has significantly weakened pri-

vacy law in this province to facilitate the B.C. Services Card and related interlinked data-tracking systems, with no clear or persuasive rationale. Where is that leading?

In Britain today, there are systems that integrate data from social services, health, policing and schools. Children and families cannot exist outside the control of a virtually all-seeing government. Is that the kind of society that you want to help create?

Just imagine a government that is slightly nastier or more ideologically driven by ideas about race or class or crime or mental health or welfare or rebellious tendencies. Once in place, how will that kind of system be used by such a government? Do the purported future benefits really outweigh the risks? Not according to the government's own citizens committee.

What should we do? I'll start by comparing this province's situation to one that is in utter collapse: Canada's federal information and privacy laws. These examples are doubly relevant because British Columbia seems to be gradually moving towards the federal model.

Essentially, the Office of the Privacy Commissioner of Canada and the Office of the Information Commissioner of Canada have investigative powers but little in the way of meaningful enforcement powers. So there's an ever-expanding list of cases where the OPC and the OIC have found that information and privacy laws are being broken, and they haven't been able to do anything about it.

Not long ago, for example, the federal Information Commissioner went public with her complaints that the RCMP is regularly breaking information access laws, including simply ignoring access requests for years on end and destroying information. Health Canada is notorious for stonewalling requests for years. In both cases, access requests of my own were involved.

[0945]

Similarly, the Privacy Commissioner has publicly identified programs at federal agencies that are in breach of privacy law but has not been able to prevent or stop them.

Here in B.C., we have many of the same problems. I've had tiny information requests take years. However, unlike those federal offices, the OIPC also has some actual order-making powers. The commissioner can, in some circumstances, force an agency into compliance with the law. Even when that power is not used, it helps significantly that it is there as a caution and a warning.

My main frustration is that we too often aren't even enforcing the laws we have now, which at least are better than the federal ones. In my opinion, FIPPA would be much better if it provided broader powers to proactively monitor, enforce and administer penalties. I'll give some examples.

A couple of years ago, I discovered that many public schools in the Western Communities just west of Victoria had installed surveillance cameras outside and inside the schools. The school board had even authorized the use of cameras in children's washrooms, and they would allow access to the saved video feeds. I started asking questions.

The last I heard, the school board had at least begun communicating with the OIPC about coming into compliance with the law. But it's an apt illustration of how these kinds of things are just happening around the province without oversight. We need proactive monitoring of what's going on out there. Incidentally, the B.C. government has passed legislation specifically giving schools more ways to bypass FIPPA.

Another example. I discovered that the city of Vancouver's downtown surveillance cameras and saved video feeds were routinely being used in contravention of the city's own publicly stated policies, and it had been going on that way for years.

Another example. B.C. municipal police boards are supposed to provide a level of open citizen oversight on the police. Police boards are, therefore, required by law to give reasons for going in camera at meetings and to provide the uncensored minutes to the Ministry of Justice in confidence. The Justice Ministry has refused to answer my questions as to whether anyone actually ever reviews those reasons and determines whether they are reasonable or not. Are B.C. police boards routinely breaking the law? We don't know. We need proactive monitoring and enforcement.

Another example. Not long ago, B.C. police were building a program of mass surveillance called automatic licence plate recognition, modelled after similar programs in the U.S. and U.K., where a mix of stationary and police car–mounted cameras constantly snap photos of every single car on the roads and store information about the licence plate, the date and time and the precise location of every vehicle. Over time, this builds an astonishing database of information about every driver's whereabouts at all times.

I, a technology expert and a privacy expert investigated this and discovered that the system was operating in contravention of B.C. law, plain and simple. It was an illegal surveillance program gathering information on the activities of innocent citizens and being run by our own police forces. We presented evidence to the OIPC. They decided to investigate, and sure enough, the OIPC found that the program was illegal.

Notably, we also learned that both federal and B.C. commissioners had reviewed and expressed concerns about that program in the planning stages, but neither had the legal authority to prevent the program. We need to proactively monitor and enforce the laws that are on the books.

Another example. The buying and selling of information about people and their activities is a multi-billion-dollar industry in North America, and it's growing rapidly. Privacy data breaches and identity theft are becoming more common, and they can and do destroy people's lives. There needs to be more proactive monitoring in that area as well.

Subsidiaries. This issue has been brought up to you repeatedly, so I won't go into it here, but I'm certainly in agreement that subsidiaries of public institutions should be held accountable under FIPPA.

Erasing history. We clearly need a law more strongly outlining a duty to document in the public service and penalties for breaking FIPPA. I'm sure you've heard a great deal on that issue. I, too, have seen many cases of government workers deliberately not keeping or illegally erasing or conveniently not finding important information that was subject to an access request. I've read e-mails where senior bureaucrats were instructing others to delete important e-mails. You can see examples of these sitting on the B.C. government's Open Information website.

To be clear, I'm not saying that it's the common practice of average public employees. On the contrary, in my experience, most average public employees are proud of their work and want their work properly recorded, filed and known about by the public.

[0950]

From what I've seen, the directives to not keep records, to miss records and to delete records are usually politically motivated, and they emerge from the most senior personnel within the public service that are working the most closely with elected politicians. That's why I was not surprised to see the recent revelations about those kinds of actions happening in the Office of the Premier.

If you feel any inclination at all to defend such practices, I ask you again: please, just imagine a situation where we have a government in power that you personally are less sympathetic to. How would you feel about it then? Are you sure this is the kind of society you want to help create?

Now I want to spend the rest of my time on an issue about which I am particularly knowledgable. It is a request for a very specific, small, but extremely important change to FIPPA. In an April 2014 letter to the B.C. government, Information and Privacy Commissioner Elizabeth Denham recommended that the British Columbia Association of Chiefs of Police and the British Columbia Association of Municipal Chiefs of Police be declared to be public bodies and be added to schedule 2 of FIPPA by an act of legislation "at the earliest opportunity."

Are you aware of this? Why hasn't it happened? Perhaps in our question-and-answer session, some of you will comment on this. I am also curious to know if anyone representing B.C.'s municipal police chiefs has presented to this committee. During past reviews, someone has always come to make arguments about ways in which B.C. municipal police should not be subject to FIPPA.

What's interesting, though, is that the police chiefs do not do it themselves — most likely because it's not something that most police boards would authorize their chiefs to do. As representatives of the public interest, most police boards, I think, would not want to be publicly seen as setting out to make their police departments vastly more secretive. So someone else often does the presentations to this committee.

Who? Well, that's an interesting question. Let's go to the *Hansard* record to find out. On January 21, 2004, a man named Volker Helmuth presented to the committee reviewing FIPPA. He began: "I'm the information and privacy coordinator for the Vancouver police department, but I'm appearing today on behalf of and as representative of the British Columbia Association of Municipal Chiefs of Police." He spent most of his time arguing why municipal police shouldn't be subject to FIPPA.

During the Q and A, MLA Joy MacPhail said to Mr. Helmuth: "I will start by saying that I'm taken aback completely by your presentation. First of all, could you tell me why this letterhead is of Jamie Graham, the chief constable?" — of the Vancouver police department — "Is he the head of the association or something? I'm sorry, I don't…."

The confusion that Ms. MacPhail is experiencing is important and telling. She is wondering why a staff member of a municipal police department is giving arguments to a legislative committee about what municipal police departments supposedly want, while he is actually representing a private lobby group, but then is providing these arguments on official municipal police department letterhead.

Ms. MacPhail is wondering who exactly this person is speaking for. Who is paying him? She never gets a clear answer.

I've been writing about these two associations, the B.C. Association of Municipal Chiefs of Police and the B.C. Association of Chiefs of Police, for several years. After my long information-access battle to get copies of at least some of the minutes of their meetings through a roundabout route, I immediately started to express my concerns and provide evidence to the OIPC.

A number of other organizations, like B.C. Civil Liberties, the B.C. Freedom of Information and Privacy Association and Pivot Legal, have reviewed the evidence and expressed their concerns to the OIPC as well. That is what led to the OIPC looking into the issue. Ultimately, the commissioner made her recommendation to government that the associations should be declared to be public bodies and added to schedule 2.

That's partly because, 11 years later, today, that same confusion that Ms. MacPhail was experiencing still exists, and the commissioner's recommendation is an attempt to clear up the confusion. No one really knows what these associations really are or who they really represent.

However, they are extremely important and influential in matters of public policing in B.C. What I can tell you is that they both claim to be private groups not subject to FIPPA. Yet what I can also tell you is that both associations often claim to officially represent public police forces in this province.

They make many policing governance decisions; help craft legislation for the provincial government; share

highly confidential policing information that often travels overseas; appoint policing representatives to important public agencies; and along with senior B.C. policing and security personnel, include among their members official representatives from the B.C. Ministry of Justice, CSIS, Canada Border Services, the U.S. Secret Service and the U.S. Drug Enforcement agency.

It does sound like a collaboration of public bodies, doesn't it? But their meetings and decisions are not subject to FIPPA?

[0955]

Meanwhile, both associations also claim to be simply comprised of private citizens in a private group. One of them includes members who represent private sector companies, and they engage in activities like fundraising for their group, lobbying, and public relations activities on controversial matters of public policy, like federal surveillance legislation and changes to FIPPA.

The upshot of this confusion that Ms. MacPhail was intuitively wondering about is, for example, that the police officer members of the B.C. Association of Chiefs of Police take money from the Canadian Bankers Association to further the goals of their private group. And at the very same meetings, they make decisions about how to improve official police responses to crimes at banks.

Stay with that. Yes, that's me cutting a cheque to support your bowling team and you, during that same meeting, committing to support legislation that creates new grants for freelance journalists like me. That's about as blatant an example of inappropriate conflict of interest in public servants as could be dreamed of. Most police agencies have policies forbidding such practices, but these organizations are not transparent to the public, and they function without accountability to the public.

Both the B.C. Association of Chiefs of Police and the Association of Municipal Chiefs of Police need to be added, via legislation, to schedule 2 of FIPPA and made appropriately subject to FIPPA, as our public police departments and police boards are. This is necessary so that you as our elected politicians, B.C. police boards and B.C. citizens at least have a window into how our police are being governed in this province.

It is vital, too, for the Ministry of Justice to draft legislation to ensure that the governance of policing in B.C. is properly under the control of government and not under the control of two private groups. But if the Justice Ministry is going to continue to avoid doing the right thing, then hopefully at least being exposed through the window of FIPPA will help push these public employees to do what's right.

You can do what's right. Add these police chief associations to schedule 2 of FIPPA.

D. McRae (Chair): Thank you very much. We have up to 13 minutes for questions.

D. Eby: Thank you, Mr. Wipond, for coming. It's nice to put a face to the name.

Can you advise what the context was for the commissioner's recommendation around these two associations that you're recommending be added to the schedule for the act? Why was the commissioner engaged with that? What was the context for that recommendation?

R. Wipond: Largely, for some of these things I'm pointing out to you, we had gone through a process of trying to find out…. I was trying to find out what these associations were up to. They declared themselves to be private groups not subject to FIPPA. Mediation occurred, and all sorts of evidence started to gather. I just basically started passing information to the commissioner's office, saying: "I think you should look into this, because what we're talking about here is what looks to me like a public body operating outside the auspices of FIPPA."

It was within her jurisdiction to look at it. She looked at it, and she invited submissions from anyone. Both the associations submitted. I submitted. Some of the private, non-profit groups I mentioned submitted. And then she made a recommendation.

In her letter, which is on her website and available to all of you to see, she not only makes her recommendations but includes all of our submissions as well. It's a very educational document. You see that the associations do not resist the idea of becoming subject to FIPPA, but neither do they endorse it. I don't know why it hasn't happened. No one actually said they shouldn't be, but it still hasn't happened.

D. Eby: I can advise you…. I'm not aware that we have had any presentations from the chiefs of police or from any municipal police departments, but it may be useful for us to hear from them on this point.

The second question I have is in relation to the B.C. Services Card input that you mentioned. What, specifically, coming out of that B.C. Services Card input would you recommend that this committee focus on in terms of our potential amendments recommended to the Legislature?

R. Wipond: Oh, gosh. I'd just say you've got to read it. Really, I'm not an expert on that particular thing. B.C. Civil Liberties, I think, has been looking at that a lot and would provide great input on that. But I just found that it really, most importantly, impressed upon the government the significance of what was happening and the importance of getting it under control. I had some concern that that didn't seem to be followed.

[1000]

K. Corrigan: Thank you for your presentation. I notice that with regard to the automatic licence plate recognition program, you say: "We also learned that both feder-

al and B.C. commissioners had reviewed and expressed concerns about that program in its planning stages, but neither had legal authority to prevent the program."

Was that an opinion that was expressed by the commissioner — that there is no authority to proactively take a look at actions of government until there is a complaint afterwards?

R. Wipond: That's not an opinion they've given. As far as I know, that's the way it is. That's the law. They just simply try to coerce and pressure and suggest. They go into public venues and express their concerns — sometimes later, if the thing keeps continuing. Essentially, they don't have that authority. I found documented evidence, at length, of them expressing some of the same concerns that we ultimately had and that were ultimately proven to be illegal.

D. McRae (Chair): Are there other questions from the committee?

Thank you very much for your presentation, sir. Like it was said earlier, your presentation, obviously, goes into *Hansard* on record, but if you wish to add a written submission, we'll take that up to January 29 of 2016.

If I could ask the committee to take a short recess for two minutes, and we will resume. We're going to be joined by the regional district of Central Kootenay via video conference. We'll recess for two minutes.

The committee recessed from 10:01 a.m. to 10:06 a.m.

[D. McRae in the chair.]

D. McRae (Chair): We are now being joined via video conference by Bronwen Bird from the regional district of Central Kootenay.

Bronwen, we haven't used this technology a lot, but we've done it a couple of times. Hopefully, you will be able to see and hear us. We can see and hear you. By practice of the committee, we'd ask for a 20-minute presentation, if that's what you have. Then that would allow committee members ten minutes to have questions and answers for further follow-up if necessary.

I'm a little congested today, but I will do my best to run a meeting on time. According to my watch here, it is 10:07, and I will turn the floor over to you.

B. Bird: Good morning. Thank you for this opportunity to speak. My name is Bronwen Bird. I'm the records and information management analyst for the regional district of Central Kootenay.

Our head office is located here in Nelson, B.C. The RDCK is responsible for providing services such as building inspection, land use planning, waste and recycling, recreation services and many other services to the Central Kootenay region. In my role, I'm responsible for implementing a records management program for the RDCK as well as processing the freedom-of-information requests that we receive.

I'm going to begin with what I view as the most pressing issue regarding freedom of information in B.C., which is the duty to assist. Section 6 of the act states: "The head of a public body must make every reasonable effort to assist applicants and to respond without delay to each applicant openly, accurately and completely." This section is very clear, and in my opinion, it captures the spirit of the act, which is to make public bodies transparent and accountable and to provide information to the public without unnecessary delay.

However, this duty to assist is not always upheld. I'm going to briefly describe an experience that the RDCK had earlier this year with a provincial ministry. The RDCK made a request for records on February 25 of this year, and this ministry responded the next day to acknowledge our request and to inform us that the 30-business-day time limit was April 10. It was a fairly large request. So I was prepared that the ministry might require a time extension to respond.

A month later we received a fee estimate, which we paid. Another month later, on April 29, we received another fee estimate, which we also paid. At this point, we requested an update on the timeline for the request, since they had exceeded the 30-business-day time limit and they had not informed us of taking a time extension under section 10. We received no response to this request for an update.

Another month later, on May 21, we requested again for an update on the timeline. The response that we received from the ministry was that they went past the due date because of an administrative error. We made a complaint to this ministry the next day, requesting an explanation of this administrative error, and once again we requested details on an expected time frame for the release of records.

Another month later, on June 22, we had to remind the ministry that we were expecting a response to our complaint. The ministry informed us that the administrative error was that they did not take an extension under section 10 and that they hoped to send records to us soon. As well, they would waive the remainder of the fee.

[1010]

This is now four months since we submitted our request. We had paid two fees, and we still had no records. At this point, we made a complaint to the Office of the Information and Privacy Commissioner.

The OIPC office told us that the ministry would send us records by July 3 at the latest. We did not receive a response by this date, so our file was transferred to an investigator. We finally received the records we requested on July 6.

Once we received the records, our OIPC file was closed, because the only issue with our complaint was the min-

istry's failure to respond to our request. Since the ministry eventually responded to our request, albeit 59 business days late, the OIPC considered the issue to be resolved, and there was no reason to continue the investigation.

As I'm sure you can imagine, this situation was very frustrating for us. It was frustrating to witness the ministry's blatant disregard of their duty to assist and to inform us of the time limit extension. But what was most frustrating was that even though the ministry was 59 business days late in disclosing the records to us and we had paid two fees, our complaint file was closed once we received the records, and there was no consequence to the ministry.

There needs to be a consequence for breaching the act. I'm sure the RDCK's experience with this ministry is not unique, and if public bodies are allowed to take unwarranted extensions and fail in their duty to assist, it completely undermines the act and the concepts of transparency and accountability.

In the 2010 report of the special committee, several submissions had brought up this issue about public bodies making a reasonable effort to assist, and those submissions proposed penalties. Despite these submissions, the special committee did not recommend imposing penalties, but rather, it felt that it is more important to waive fees to provide some kind of incentive for heads of public bodies who breach the duty to assist.

I feel that this decision should be reconsidered and that a recommendation for penalties be implemented if a public body does not make every reasonable effort to assist applicants. Waiving fees is not an adequate incentive for public bodies to not breach the duty to assist. In fact, I believe that by only waiving fees, there really is no incentive at all for public bodies to not breach the duty to assist. What about requests that do not incur a fee, such as requests for an individual's own personal information or a request where the fee is small? Where is the incentive to respond to those requests?

Penalties against public bodies for breaching freedom-of-information legislation is not an uncommon thing. This is seen in the freedom-of-information legislation of several countries around the world — for example, Serbia, Slovenia and Croatia, to name only three. The legislation of these countries and others imposes fines against public bodies for a misdemeanor, such as failing to communicate accurate and complete information, failing to provide the public information requested within the prescribed time limit, as well as destroying or concealing records with the intention of making such information inaccessible to the public.

B.C. should follow the example of these countries and the many others that have penalties for breaching freedom-of-information legislation. There could be set fines, or there could be a fine for each day beyond the day that the request should have been responded to, not exceeding a determined amount. Penalties such as this would be a much stronger incentive for public bodies, including provincial ministries, to respond to requests without delay and to uphold the act. I urge the committee to seriously consider penalties because it is clear that merely waiving fees isn't working.

My second point regards the time limit for responding. The 30-business-day time frame should not be changed. I can see how some people will view the 30 business days as a long response time, especially if there are further time extensions. However, for some cases, this time frame is perfectly adequate, especially for large and complex requests. I have processed requests where there are several hundred pages of responsive records. It takes time to read through those pages and make decisions on whether information needs to be severed.

Speaking from my own experience, there are also times when you are processing multiple FOI requests at the same time. For some requests, they can be processed very quickly — in a day or two, maybe a week — but this is not the case with all requests.

Furthermore, if there is information that could be harmful to personal privacy or third-party interests, the affected parties need to be notified, which takes additional time.

I feel like it comes down to public bodies making internal policies and procedures about responding to FOI requests and having adequate training and resources to ensure timely responses as opposed to changing the response time in the act. So long as public bodies are abiding by their duty to assist, then timely responses shouldn't be a problem.

[1015]

Problems with time limits arise when public bodies fail to make a reasonable effort to assist applicants of FOI requests. It is this lack of reasonable assistance which is the problem that really needs to be fixed.

A possible solution is what I mentioned before, which is penalties for public bodies. Without adequate consequences, it feels like public bodies are sometimes able to get away with it, when it comes to taking extensions and disregarding time limits.

My third point speaks to the relationship between records management and freedom of information. Timely responses to freedom-of-information requests are dependent on good records management. Proper records management can help with locating and retrieving records, reducing fees and allowing public bodies to process the requests quicker rather than wasting time trying to locate a record.

I've experienced this myself, in which the bad records management practices of 20, 30, even 40 years ago have affected my ability to respond quickly to an FOI request. I've had to spend several hours going through poorly organized microfiche slides from 30 to 40 years ago, and I've had to search through several boxes of poorly labelled files from 20 years ago trying to find a responsive record.

You can imagine my excitement when I found the records I was looking for — but not without much difficulty. It's because of these difficulties that I'm very glad to be implementing much better records management practices here at the RDCK. Just like other public bodies, we do still have a ways to go, but we're implementing changes that will benefit us as well as the public now and into the future.

However, based on reports such as the recent OIPC report on the deletion of e-mails in the provincial government and the lack of documentation, it is clear that records management practices need to be improved significantly.

This includes documenting business activities, organizing and filing records according to a clear and usable filing system, and retaining records according to an approved retention schedule, only deleting or destroying records that have reached their final disposition and there are no further actions, including being responsive to an FOI request, that require those records to be kept.

The act should require public bodies to properly maintain their records, cataloguing and indexing them in such a way that it facilitates the right of access to information.

I agree with the B.C. Freedom of Information and Privacy Association, who presented in Vancouver last month, that there should be a duty to document and retain records. This point was also brought up by Laura Millar, who presented in Vancouver last week. She used the example of the State Records Act of the government of New South Wales in Australia, which requires governments to create accurate records and retain those records as long as required.

Recordkeeping requirements are also seen in the freedom-of-information legislation of other countries, such as India, Antigua and Barbuda, for example. B.C. would do well to follow their example.

My final point speaks to proactive disclosure. The benefits of proactive disclosure are plentiful. It promotes accountability and openness. It provides the public with access to information that allows them to participate in the decision-making of public bodies. It also encourages public bodies to manage their records and information more effectively and helps with reducing the amount of requests for information by routinely providing information that can be easily provided without a formal request.

According to section 71 of the act, "the head of a public body must establish categories of records that are in the custody or under the control of the public body and are available to the public without a request for access under this Act."

However, without a minimum standard of what these categories of records are, the standards for proactive disclosure will vary widely across public bodies. Some public bodies will be very thorough in establishing categories of records, whereas others may only establish a few. There should be a minimum standard established which details the classes of information that should be proactively disclosed by public bodies.

This could include policies, descriptions of services offered to the public, budget and other financial information, information on public procurement processes, publications and information about open meetings. Furthermore, this information should be easily accessible on the websites of public bodies.

The RDCK currently puts information such as financial reports, bylaws, open meeting minutes and other documents on our website, and we will continue to work on proactively disclosing records. But there would be a great benefit to having a list of records and information prescribed by the act that must be proactively disclosed by all public bodies and be organized in a meaningful way.

[1020]

Additionally, there should be requirements in the act for public bodies to proactively disclose accurate and complete information, unless information can be withheld under the act. This information should also be regularly updated within a reasonable amount of time to remain accurate and valuable to the public.

In conclusion, I feel like B.C. still has a ways to go to ensure that the ideas of transparency, accountability and open government are not just words but the reality of how our public bodies operate. I feel like many citizens make FOI requests already thinking that they're going to face delays and will receive records with half the words blacked out, if any records at all.

If you look at the freedom-of-information audit from this year that was prepared for Newspapers Canada, you can understand why this sentiment exists. The audit shows that at all levels of government across Canada, several public bodies received poor or failing grades for the release of information and the timeliness of response. Furthermore, this sentiment isn't helped by recent media stories, such as the OIPC's report on the deletion of e-mails in the provincial government, particularly e-mails that responded to a request about the Highway of Tears.

Overall, I do believe the act is strong and sound. The problem is mainly with the failure of public bodies to follow the act and the failure to uphold the spirit of the act. Public bodies should not be allowed to take unnecessary extensions and charge exorbitant fees. Public bodies should not disregard their duty to assist and should face penalties if they do so.

My hope is that the special committee will make strong recommendations that will address the many issues that have been brought up today, as well as in the past meetings regarding the act, and that these recommendations will result in meaningful changes. As well, I hope that B.C. will become a standard of excellence for freedom of information, both in Canada and internationally.

To summarize my recommendations to the special committee, first, the act should be amended to include

penalties against the head of a public body for breaching the duty to assist. Second, the time limit for responding should remain at 30 business days. Third, the act should be amended to include recordkeeping requirements, including the duty to document and retain records. Finally, the act should be amended to include a list of classes of information that should be proactively disclosed by public bodies. Proactively disclosed information should be complete and accurate, organized in a meaningful way and regularly updated.

Thank you very much for listening.

D. McRae (Chair): Thank you, Bronwen. I'm sure we have some questions.

K. Corrigan: Thank you so much for your presentation. I only have one short question, but I want to make a comment first. It's really heartening to see a public body talking about the responsibilities under the act and acknowledging and supporting the fact that there are responsibilities and that government should take those responsibilities seriously. They should follow the act and stand up for the ability of citizens to be able to access information. It was great to see that we had a regional district making this kind of presentation,

Now, it's interesting that you're not only subject to the act, but you also use the act as well. Your concern was partially based on the fact that you didn't have access or you had difficulties with the request — those kinds of timeline difficulties and some of the other difficulties that you expressed. I'm sure you're aware that those are the same kinds of difficulties that we've heard repeatedly in presentations before this committee.

I'd also point out that you might be heartened to know that the submission that we're receiving today from the Information and Privacy Commissioner makes many of the same recommendations that you are making. So there you go. You and the Privacy Commissioner — or the office — agree on that.

Finally, my very, very short question was: do you mind sharing which ministry it was that you had the difficulties with?

B. Bird: It was the Ministry of Environment.

K. Corrigan: Great. Thanks for the presentation. It was very helpful.

D. McRae (Chair): That was a short question.

K. Corrigan: A long preamble, short question.

D. McRae (Chair): And a great answer.

D. Eby: The recommendation around proactive disclosure — in it, you include a short list. You say this could include policies, budget and other financial information, public procurement information, publications and information about open meetings.

Is there anything that's not in that list that you think this committee should consider in terms of requiring proactive disclosure? And then is there anything on that list that you would say absolutely should be on and is not currently regularly being posted?

[1025]

Many of the things on the list, I would say, most cities and ministries would be proactively disclosing already. Is there anything on the list that stands out for you that they're not doing and anything that's not on the list that we should think about?

B. Bird: Not exactly. I can definitely go back and compile a more detailed list and provide that to you later.

Mostly, it's information about how the public body is operating. The one thing that most public bodies probably don't include is the documents or the information that they compile in order to make a decision. They'll post…. In the open meetings, you'll have the decision, but there won't be the records that were created or used in order to come up with that decision in the decision-making process — any reports that are submitted or any other information of that nature.

D. Eby: If you could provide that list, that would be helpful to us in our deliberations.

B. Bird: Definitely. I believe I have until January to submit information. Is that correct?

D. McRae (Chair): January 29, 2016. We have your submission already, but if you wish to add to it, by all means, we would like to take that information.

Are there other questions from the panel members?

Bronwen, thank you very much for joining us via teleconference. Enjoy your time in Nelson.

D. McRae (Chair): We are moving fast and furious. I notice that staff from the Ministry of Technology, Innovation and Citizens' Services have joined us. I know we're a little bit ahead of schedule, but if they're willing, we can start early.

I'll take a recess for maybe one minute to allow them to get organized and for everybody else to stretch their legs.

The committee recessed from 10:26 a.m. to 10:30 a.m.

[D. McRae in the chair.]

D. McRae (Chair): Ladies and gentlemen in the audience and at home, we are being joined by the Ministry of Technology, Innovation and Citizens' Services for their second visit to the committee.

Before we begin, though, I would like to just address one issue. About three weeks ago, if my memory is clear, I received a letter from Minister Virk regarding some recommendations. As Chair of that committee, I then shared that letter with all members of the committee and the Clerk's office. We have it in our files. However, we take it as part of the submission from the ministry.

At this stage, if it's possible, I would like to invite Bette-Jo to introduce yourself and the staff who are joining you, although we've met you before. Also, I'll just remind everybody that we have scheduled 30 minutes for this presentation and 30 minutes for questions and answers, if they so happen afterwards. Again, welcome to the committee.

Full disclosure. I get tired of saying it, but I am ill. I'm going to stay as far away from as many people as I possibly can, except for poor Susan, who has to sit beside me the entire time.

B. Hughes: Well, thank you, Mr. Chair. Unfortunately, I'm probably sharing the same bug. I apologize if I passed it on to you at the privacy conference last week.

Thank you, Mr. Chair, Deputy Chair and all members of the committee. I'd like to thank the committee for the opportunity to present to you today. As the Chair mentioned, my name Bette-Jo Hughes, and I am the government chief information officer and an associate deputy minister with the Ministry of Technology, Innovation and Citizens' Services.

With me today are two of my colleagues. To my right is Sharon Plater, who is the executive director of our privacy and legislation branch and a recognized subject matter expert on the Freedom of Information and Protection of Privacy Act. To my left here is Wes Boyd, the assistant deputy minister who is responsible for information access operations.

I'm particularly honoured to have been selected as the spokesperson to present government's views on how the Freedom of Information and Protection of Privacy Act is working and, perhaps more importantly, where we see opportunities for improvement.

Government is excited to contribute to this valuable process and looks forward to hearing the views of the committee, as well as other interested stakeholders, on how we can continue to build and enhance this legislation, given the solid foundation we have set thus far.

In preparation for its submission, government undertook consultations with all ministries and Crown corporations. The views I will be presenting today are the result of government's analysis of that input, along with its determination and assessment of the key challenges, opportunities and priorities that exist.

I'll just take a brief moment to outline what we plan to discuss on the agenda here today. Before I do that, however, I would like to advise the committee that government will be providing a formal written submission in addition to the presentation I am providing today.

One of our goals today is to set the stage and context for the committee with respect to what our current environment looks like and the impacts and influences on information and privacy. I will be touching on data residency. We know this is of key interest to many public bodies, including the broader public sector, who continue to grapple with perceived limitations stemming from the privacy act provisions.

Our goal here will be to highlight a new optimism in terms of B.C.'s place in the global and international privacy community. I will be providing an update to our access-to-information environment, and by doing so, we hope to provide some insight into how this landscape influences our understanding of what access really means in today's digital age, particularly as we look to the availability of metadata.

Government is committed to maintaining and enhancing privacy standards to address some of the issues presented by these new challenges and has ideas for ways that balance can be achieved by increasing mechanisms that will allow for greater proactive disclosure.

Next on the agenda, we are going to cover privacy in greater detail and, in particular, government's current vision on how privacy can be strengthened. We are particularly proud and excited about the launch of the privacy management accountability program or PMAP, as we refer to it. We feel that this policy, along with some key legislative amendments, will go a long way to getting us closer to where we need to be.

Finally, I will cover some much-needed housekeeping changes to the legislation.

As we have heard time and again — and as, I'm certain, others who have already presented or will be presenting or submitting to the committee can attest — FOIPPA remains an essential piece of legislation that underpins our democratic rights and freedoms.

[1035]

Government plays an important role with respect to ensuring the legislation works effectively and achieves the right balance between providing seamless and timely access to government records and information while securing and protecting personal privacy.

Finding this balance is becoming increasingly difficult in today's technological environment, with the vastness of data and information available to us, the speed at which it is created and challenges faced in securing and protecting data as it goes through necessary information-sharing channels.

Government has the willingness and knowledge and is eager to build on the tools it has at its disposal, as well as seeking out new frontiers to meet this challenge and achieve this balance. We have the ability to look to our international partners, both in industry and government, for best practices. New international standards around information, privacy and security are setting increasingly high bars for data protection, while at the same

time, leading technology firms are implementing measures that go beyond what any government is able to do.

It is my sincere hope that today's presentation will give the committee some understanding of the key challenges we face and provide you with some insightful suggestions that you can take away and carefully consider as you prepare your final recommendations.

Speaking to data residency. In 2001, the United States enacted the U.S.A. Patriot Act, allowing the FBI to conduct electronic surveillance and oblige American companies with offices in countries like Canada to provide access to sensitive personal information. Obviously, this generated quite a stir in the privacy community, as it meant that any entity using American data services became vulnerable to these new authorities.

In response to these concerns, FOIPPA was amended in 2004 to include a robust set of data residency requirements, with the aim to ensure that B.C.'s personal information remains outside the grasp of foreign law enforcement. As many of you are aware, these requirements establish that a public body must ensure that personal information in its custody and under its control can only be stored, accessed or disclosed within Canada unless specific conditions are met, as outlined in the act. These data residency provisions help to ensure that the Patriot Act and any similar legislation do not negatively impact the privacy of British Columbians.

Many within ministries and the broader public sector, however, have noted that it is at times challenging to take advantage of new and emerging technology available outside of Canada. As public bodies are required to ensure data remains within our borders, FOIPPA-compliant services that meet the unique needs of some public bodies can be scarce.

I am often challenged, both by public and private sector colleagues, regarding what some see as the overly restrictive data residency obligations in B.C.'s FOIPP Act. I do not believe that we need to reduce our legal requirement to protect the personal information of British Columbians in order to take advantage of advances in technology and cloud-based services, as long as the appropriate safeguards are in place.

As a matter of fact, Canada is witnessing an increase in the number of corporate entities who are willing to accommodate our data residency provisions in order to do business.

Maintaining the data residency provisions will assist B.C. in remaining an attractive business partner to other jurisdictions by ensuring our privacy standards continue to meet those of our peers, such as the European Union, whose data protection directive has set the bar for privacy internationally.

This year, the safe harbour agreement, which allowed U.S. companies working in Europe to self-certify their compliance with the EU data protection directive, was ruled invalid by the EU Court of Justice. This ruling is likely to have a significant impact on thousands of U.S.-based companies who relied on this agreement to do business in Europe.

The court's dismissal of the safe harbour agreement is a strong signal to the rest of the world that the EU is serious about upholding their data protection standards at all costs. In that light, B.C. must ensure that our FOIPP Act remains on par with global privacy leaders to remain a viable partner in business and trade.

Government remains assured that B.C.'s current data residency provisions provide an effective level of data protection in a continually evolving technological environment. These provisions not only align with the EU's public sector data protection directive but also match — and in many aspects, exceed — current standards, such as ISO 27018, which set the bar for the private sector in the realm of cloud computing.

[1040]

Moving on to access to information, it cannot be denied that B.C.'s population is active when it comes to exercising its access rights. We think this is positive in that it greatly contributes to ensuring that the legislation remains relevant to the citizens of British Columbia.

The B.C. government receives between 8,000 and 10,000 freedom-of-information requests per year. The total cost of processing an FOI request is approximately $2,300 per request. The number of general requests has increased more than twofold since 2008-2009, when government centralized its freedom-of-information services.

In 2013-14, we fulfilled more freedom-of-information requests than all of the prairie provinces combined in that same year. We received 30 times more requests than the Newfoundland and Labrador government ministries. Compared to a larger province like Ontario, the B.C. government receives twice as many requests per capita. These statistics are particularly significant when set against the digital environment and landscape I mentioned earlier.

All large organizations, including governments, manage the steady increase of information with comprehensive IT systems. From e-mail to case management software, these systems help government run as efficiently as possible.

As a by-product of the many data functions these systems perform, a massive amount of metadata is produced. Metadata is data that describes other data and is used to summarize basic information, such as the author, the date and time an item is created or modified or the location of a file or folder. While this metadata is very useful for system evaluation and maintenance, its availability in large quantities poses a new problem for government.

Though once considered benign to many, metadata found in government e-mail and server logs is beginning to generate interest from knowledgable freedom-of-information applicants who file requests for these logs spanning large time frames. A responsive records

package for one of these requests can include millions of lines of data, which public bodies must process and prepare for disclosure.

More concerning is the prospect of freedom-of-information applicants using this data in combination with other data that is readily available through social media and other sources to undertake surveillance of the habits of government employees. This is referred to as the mosaic effect, which a former commissioner's order described as when seemingly innocuous information is linked with other already available information, thus yielding information that is not innocuous and, in the access-to-information context, is excepted from disclosure under the act.

In the March 2015 investigation report into the use of employee monitoring software by the district of Saanich, the commissioner states that "employees do not check their privacy rights at the office door" and that these rights "must be respected by public bodies as they consider what security controls are necessary to protect information in government networks."

What is the solution, and how can we ensure that delicate balance between privacy and access is maintained? As with any piece of legislation that has been in existence for some time, I think the first step is acknowledging that perhaps, in its original crafting, the legislation never contemplated the technologies and data available today, such as metadata.

We need to modernize and update the legislation to address the issues posed by metadata. Doing so will maximize public trust, transparency and accountability while at the same time balance the privacy rights of the individuals whose information is contained in this metadata.

Having said this, government also sees opportunities for promoting greater transparency by utilizing current mechanisms afforded within the legislation that allow for proactive disclosure. Specifically, more records could be made available via section 77.1 of the legislation, which speaks to records made available under mandatory categories of release.

Currently this provision lends itself only to those records that would otherwise be available for full release and therefore would not require redaction due to the fact that they may contain sensitive personal information. A minor amendment to this section would enable government ministries to consider the potential for proactively releasing other categories of records if they had the ability to remove otherwise sensitive personal information beforehand.

[1045]

Along these lines, section 25 speaks to the mandatory requirement for ministries to proactively release information which is clearly in the public interest. It is applicable only and appropriately reserved for proactive disclosures of a serious nature — for example, environmental or health crises which directly impact the public. The reason for this is that section 25 overrides all other exceptions to disclosure, including the exception that protects personal information.

Newfoundland and Labrador has adopted a more measured approach to the release of information that is in the public interest. This approach also requires the proactive release of information, but the information that must be released is measured against and commensurate with the nature of the exception being overridden. In particular, the bar for releasing personal information is higher than that for other types of information.

Taking a similar approach here in B.C. may provide a means of protecting privacy while still releasing information when it is clearly in the public's interest to do so.

Another improvement to access will be the inclusion of the B.C. Association of Chiefs of Police to FOIPPA. The commissioner has recommended that the B.C. Association of Chiefs of Police and the B.C. Association of Municipal Chiefs of Police be added as public bodies to schedule 2 of FOIPPA.

The B.C. Association of Municipal Chiefs of Police is not a registered society and, by extension, not a legal entity. Therefore, it cannot be covered by legislation. With regard to the B.C. Association of Chiefs of Police, government is drafting an amendment that will change the definition of a "local public body" to include a police association. This change will cover the B.C. Association of Chiefs of Police as soon as the amendment is passed and will allow the B.C. Association of Municipal Chiefs of Police to be covered once it is a legal entity.

Moving on to strengthening privacy. As I mentioned at the outset, FOIPPA provides us with a solid foundation from which we can build and continue to enhance current privacy practices. Over the last year, government has been working diligently on a comprehensive privacy policy aimed at strengthening privacy practices across government ministries and which can be leveraged by the broader public sector to help guide and encourage them to adopt similar frameworks and processes.

We are very proud to say we are finally going to see the fruits of this hard work with the up-and-coming launch of the privacy management and accountability policy. This comprehensive policy was developed with consideration of materials produced internationally and also by the B.C. Information and Privacy Commissioner.

The PMAP will enshrine in policy the requirement for all ministries to have a ministry privacy officer, and I'm pleased to report that most ministries have already appointed a ministry privacy officer in anticipation of the policy. They will be responsible for implementing the PMAP throughout every ministry. They will also be responsible for a number of tasks, which include documenting the ministries' personal information through a personal information inventory; reviewing privacy impact assessments, information-sharing agreements and research agreements; and developing ministry-specific privacy training.

Ministries will also be required to conduct privacy audits and ensure that staff who handle personal information receive annual refresher training on top of the mandatory initial privacy training required of all staff. Most importantly, the PMAP enhances ministry accountability and will make it easier for ministries to comply with mandatory assessment tools, agreements, and breach reporting and auditing requirements.

Having said this, there are nevertheless a number of key legislative amendment items that have been identified that can also further strengthen privacy practices. These include revision of the data-linking provisions, updating and clarifying the existing privacy impact assessment provisions, incorporating mandatory breach notification requirements, and streamlining and expanding the commissioner's powers and processes. I'll go through each of those in turn.

Revision of the data-linking provisions has been on both the commissioner's and government's radar for some time. Following amendments made to the legislation in 2011, the commissioner expressed concern that the provisions as currently written were not achieving their intended policy outcomes. Simply stated, it was felt that the definition of what constituted a data-linking initiative was too narrow and failed to capture the types of activities that should be subject to the commissioner's oversight.

Government embarked on extensive consultations with the commissioner's office and has developed a new legislative scheme that will meet the needs of all stakeholders.

With regard to conducting privacy impact assessments, or PIAs, these continue to be an internationally accepted best practice for evaluating and mitigating risks at the development stage of any public program, initiative or system. In 2011, we expanded and enhanced existing PIA requirements to include all public bodies and oversight by the commissioner.

[1050]

Nevertheless, over the course of time, a few clarification issues have come to light. These include a lack of explicit authority for the minister responsible for the act to direct ministries to carry out and submit PIAs; a lack of clarity that ministries must do PIAs on current enactments, systems, projects, programs and activities, where directed by the minister, and all changes to these initiatives, including expansions of data-linking initiatives; a lack of clarity that ministries must inform the minister responsible for the act of new, or changes to existing, information-sharing agreements and personal information banks for the purpose of inclusion in the personal information directory; and also, a lack of clarification that only one PIA need be done if several public bodies are involved in data linking. Government is ready to propose changes to the legislation that will effectively address these issues.

Moving on to mandatory breach notification requirements. A number of high-profile privacy breaches reported within government over the years have placed a spotlight on the issue of privacy breach management. While it can be acknowledged that information incidents can, ultimately, never be eliminated entirely anywhere where the potential for human error exists, strengthening proactive measures that mitigate the potential for such incidents to occur in the first place is the best way to tackle this issue.

As you may be aware, both the 2008 and 2015 special committees that reviewed the Personal Information Protection Act, or PIPA, B.C.'s private sector privacy legislation, recommended that mandatory privacy breach notifications be incorporated into PIPA. The commissioner is supportive of this recommendation and has asked government to enshrine mandatory breach notifications within FOIPPA as well.

Government already provides monthly reports to the Office of the Information and Privacy Commissioner about each privacy incident investigated by the office of the chief information officer. When we become aware of an incident that is considered a serious privacy breach, government continues to report directly to the commissioner.

Obviously, the biggest impact with such a requirement will be felt by the broader public sector bodies, which may not have the same reporting practices and infrastructure. Government has committed to addressing the mandatory breach notifications within PIPA at the next available legislative opportunity and welcomes any similar recommendations in this regard with respect to FOIPPA as a means of maintaining harmony between both pieces of legislation and meeting international privacy best practices.

Moving on to the commissioner's powers and processes. Both the 2004 and 2010 special committees to review FOIPPA recommended that the commissioner's processes be unified and streamlined in order to provide greater clarity and accessibility for the public as well as allow for operational efficiencies for the commissioner's office. The commissioner has expressed support for a revamping of the act's provisions respecting these processes and, in particular, has called for harmony and consistency with PIPA with respect to these provisions.

The proposed changes aim to resolve ambiguities stemming from terminology for dealing with complaints, reviews and investigations where these respective terms appear to be interchangeable, overlapping and inconsistent. In addition, while the commissioner can require public bodies and organizations to stop collecting personal information or fine ministries for violating data residency provisions in FOIPPA, the commissioner cannot impose a temporary or definitive ban on the processing of personal information by a body, which is a power that many of her counterparts hold in other jurisdictions such as the European Union.

Amendments to the legislation would resolve these issues by clarifying and consolidating the commissioner's processes for investigating complaints and conducting reviews, and the terminology used to describe those processes; provide greater flexibility with respect to applying dispute resolution methods best suited to the issues at hand; and expand the commissioner's oversight with regard to personal data-processing compliance issues, which will serve to better align FOIPPA with other leading global privacy legislation.

Moving on to some housekeeping changes. As with any large and complex piece of legislation such as FOIPPA, and particularly one that has undergone a number of changes, it is only natural that over the course of time, minor adjustments are required to rectify ambiguities and inconsistencies in terminology and language that only become evident upon close examination and application of the act. We have accumulated a number of such housekeeping changes, the majority of which have been identified by government solicitors. These amendments are too numerous and minor in nature to go through in great detail here with you today.

[1055]

However, we will propose to provide you with a listing of these changes that we will append to our formal written submission. To give you an example, they can include rectifying inconsistencies respecting the interchangeable use of terms and language, such as the use of the term "public body" versus "the head of a public body" and the seemingly interchangeable use of the terms "provide access," "make available," "publish," "release" or "produce."

Finally, with regard to the commissioner's recently released investigation report, F15-03. As you know, government has hired David Loukidelis, former B.C. Privacy Commissioner and former Deputy Attorney General, to assist government in making sure that all of the recommendations the commissioner has made are properly, thoroughly and professionally acted upon across government.

We look forward to his review and recommendations and may provide additional information to the committee following his report, which is expected in mid-December.

Thank you for your attention to the information I've provided to you today. We are pleased to answer any questions that the committee may have.

D. McRae (Chair): Thank you very much.

What a surprise. We have some questions.

D. Eby: Thank you to the staff of the ministry for presenting today. First, a short question of clarification. Will you be providing a table of all of your proposed legislative amendments? There were a number under "Strengthening privacy," for example, that you talked about, as well as the miscellaneous amendments. So we'll get full table of those? Thank you very much.

I was surprised not to hear specific recommendations from you today in relation to three of the issues identified by the minister in his October 22 letter. There's the duty-to-document provision and your thoughts about the expansiveness of such a duty, the content of such of a duty, the implementation of such of a duty — anything in relation to the recommendation of maintaining deleted electronic records available for a response to access requests.

There was an additional issue around legislative oversight of information management requirements — namely, document destruction. I didn't hear anything in your presentation related to those. I do know that Mr. Loukidelis is doing this report, but will this committee not see anything from you on these issues?

B. Hughes: We have covered a number of those issues when the Information Management Act was brought in, in the spring, specifically around duty to document and oversight provisions. We have provided all of that information to Mr. Loukidelis as part of the review that he is conducting. As I mentioned, after his review is completed in mid-December, we're happy to come back to the committee to discuss those issues.

D. Eby: If I am to understand, then, your submission is that existing legislation adequately addresses the issues in the minster's letter and, I presume, in the commissioner's report, short of any recommendations from Mr. Loukidelis.

B. Hughes: I'm sorry. What was the question?

D. Eby: Are you saying the existing laws are enough?

B. Hughes: That is part of what Mr. Loukidelis will be looking at — if there are amendments that are required to FOIPPA or to the Information Management Act addressing the specific issues that were brought up in the report.

D. Eby: Obviously, of concern to the commissioner and concern to me was that act removed any penalties for document destruction, for example. I hope that Mr. Loukidelis does address those, and I encourage the ministry to consider addressing some of those issues as well.

In the commissioner's recent report, she starts off her message by saying: "Access to information rights can only exist when public bodies create the conditions for those rights to be exercised. Government must promote a culture of access, from executive leadership to front-line employees." I agree with her 100 percent. We can pass whatever legislative amendments we wish, but without that culture, it's very difficult.

Is there a way for us, through our legislative amendments, to address this problem? I believe it is a problem. You don't have to agree with me. But is there a way for us

to address culture so that people aren't, for example, as we've seen in the Ministry of International Trade, starting off all their e-mails with "this is transitory and confidential and a cabinet document"?

How do we address that culture? Can we address that culture through legislative amendment? If so, do you have any recommendations about how we can do that?

B. Hughes: I agree with you that culture is a big part of what we need to be focusing on. We have very strong legislation. We have very strong policy.

[1100]

Again, looking at the Freedom of Information and Protection of Privacy Act and the Information Management Act, what we are trying to do is to take a look at the entire life cycle of information management, from the creation of documents to the management — providing good access, providing security of personal information and, ultimately, ensuring that those records are disposed of.

What we are focusing on is looking at how we pull those different pieces together so that public servants understand how all those things relate to each other and the importance and awareness of what government information is, how those records need to be stored, how we can ensure that we provide a duty to assist applicants who are looking for information and ensure that their personal information is protected.

I do believe that we have some very good individual training and awareness vehicles to assist public servants. I think we recognize that there's an opportunity to take a more coordinated approach to all of those to ensure that people have an understanding, not just at the back end when an FOI request is coming in but at the front end when those documents are created, of what is considered government information and what the appropriate way is to maintain those records.

D. Eby: With respect, I think we've seen a massive failure of training. I don't think this…. I don't know. Maybe the folks on the other side might disagree with this, but the commissioner's report shows that for three ministries she audited, there were systemic and serious issues with non-compliance, and other FOI requests from other ministries show similar issues. So there's a very serious training issue here. I don't agree, with respect, with your assessment, based on the evidence that this committee has.

You don't have to agree with me, again, but is there an opportunity for this committee to recommend legislative amendments with respect to training and with respect to perhaps an oath or some other process that would be administered to public servants who are appointed and brought in that they understand the seriousness of not destroying records, of their duty to assist applicants — their duty as public servants?

I'm looking for some kind of recognition, at least, that there might be some opportunity for us to do that. But if we don't even acknowledge there's a training problem, then maybe we won't be able to do that here today.

B. Hughes: As you may know, we do have a mandatory requirement for privacy training. I think expanding those training requirements appropriately to cover the other parts of information management is certainly something that could be looked at.

K. Corrigan: First, an observation. Well, actually, I'll start with a question. Do we have a hard date for the report from Mr. Loukidelis? I think we do, don't we? When is that report due?

B. Hughes: Mid-December.

K. Corrigan: Will the government be then doing any further submission or written submission after that report is available in order to incorporate any recommendations or government response to recommendations that may be relevant to our deliberations?

B. Hughes: Absolutely. Once we see the recommendations from Mr. Loukidelis's review, we anticipate that we may be coming back with further information.

K. Corrigan: Okay. So when you talked about doing the written report, that written report is expected to include whatever comes out of Mr. Loukidelis's report?

B. Hughes: We are happy to take your guidance on that. We can do the first written submission based on the presentation today and do a subsequent one, if that's more helpful to your deliberations. Or we can wait and do one after the review is completed.

K. Corrigan: Either one would be fine, and they may be separate. That's fine with me. But I just think it would be really helpful to this committee if we could get a response insofar as it's relevant to this committee.

I wanted to ask about something that was related to the report that was done — it's a minor but, I think, important point — the commissioner's report on the three areas. Would it not have been possible for government and, specifically, your ministry to be flagging inconsistencies and acting proactively when it was seen through the process, before the report was done — inconsistencies in the responses that were happening from two different ministries or two different parts of a ministry?

In other words, one of the things that was pointed out in that report was that when there was a request made to two different individuals or bodies or ministries, one side of it would come out and say, "There are no responsive records," and the other one would say: "There are 128 records."

What is your role and responsibility to flag those kinds of inconsistencies and do something proactively to address them?

[1105]

B. Hughes: I'll start, and then I'll ask Wes to comment on the process specifically. Having an inconsistency between the records between two individuals is not an unusual thing. In terms of who is the person who is required to keep…. First of all, does the record need to be kept? Then secondly, who is the appropriate person to keep that record? In making those determinations, you would have different records between two individuals.

When there are questions about responsive records that come back, Wes can speak to the process that his staff undertakes.

W. Boyd: My staff are busy processing many, many records of requests for information, of course, and they do their best to reconcile or compare requests that have come in previously to new requests that come in. If a request comes in that's very similar to a previously submitted request, we'll point the applicant to that area. Perhaps it could even be posted on Open Information.

It becomes very difficult to compare in detail a new request and records that have come in to a previous request. Basically, our staff are processing the records that come in, applying the legislation, the redaction, and working with the public body where those records came from to understand what the harms are.

We're not comparing, necessarily, two sets of requests on an ongoing basis. That would be very time-consuming.

K. Corrigan: Could I have a quick follow-up on that? I don't have it up on my screen right now, but the report expressed concern about the fact that the responses were so inconsistent. It didn't seem to suggest, in my recollection, that this could be attributed to the fact that some people might have a different role or it might be a different responsibility about who collected. The report pointed to the fact — at least, assumed — that the two individuals both should have records. One did, and one didn't.

What you're saying is that there's nothing in government that in any way proactively monitors or flags times when there is such inconsistency.

W. Boyd: I wouldn't say there's nothing in place. We do our best to identify where there might be similarities. But we just work with the public body to process those requests, those records that come in.

K. Corrigan: Okay, so there's no requirement to identify whether there should be records or whatever. It's just whatever the public body provides back.

Can I just also say that I would have found it helpful…? I don't know about other members of the committee, but I would have liked to have had the full submission — apart from anything that might come up with Mr. Loukidelis.

I would have loved to have been able to do an in-depth comparison of what the commissioner is presenting today, which is a very in-depth and robust presentation, with what the government was comparing. I appreciate the overview and the verbal overview, but it would have been nice, because we're not going to have another public opportunity to discuss it.

D. Routley (Deputy Chair): Thanks to the ministry staff and officials. I have, essentially, two questions.

One of the issues that's come before previous committees and has been frequently brought to the attention of this committee is the issue of subsidiary corporations of public bodies. It has been an ongoing recommendation, which hasn't yet been answered with legislative change, that subsidiary bodies be included, particularly educational public bodies.

The former Education Minister, Shirley Bond, did acknowledge that it was a gap in the legislation and indicated that it would be addressed, but it has never been addressed. I understand that there are challenges in achieving that. Could you describe what those challenges are?

[1110]

Then the second question is around archiving. We've heard from one presenter — and I think it was a good suggestion — that more efficient archiving could streamline this process and make for more consistent responses. In other words, a consistent archiving process that would allow the anonymization of documents more expediently, rather than, perhaps, slowing down the process. The referencing of documents might be more consistent if there were more efficient archiving.

Are there any efforts being made in the ministry to achieve those efficiencies?

B. Hughes: I'll answer your last question first. With regard to having digital information that's more readily available, both for access and for archives, that is the intention of the implementation of the Information Management Act, which we hope to be bringing into force early next year.

Having all of the documents digital will allow us to use technologies to be able to find information and, if necessary, anonymize it for broader access as well as ensuring that we have a digital archive available, too, for those 3 percent of documents that need to go into archive — moving them into there.

Yes, that is part of the intention, and we are in the process of doing a request for proposals for technologies and companies that can assist us in those tools to do that.

With regard to your question around the complexities that we've heard with regard to subsidiary corporations…. Sharon, if I could ask you to speak to that.

S. Plater: We went out and spoke with the broader public sector. We didn't just speak with universities; we spoke with health authorities and other broader public sector entities.

We discovered that when you think of a corporation, you think of something fairly straightforward and simple; at least, we did. But what we found is you can have one single corporation that includes that university, other universities not necessarily within B.C., the municipal government, the provincial government, the federal government, non-profits and other corporations that are private companies — all within one single entity.

It's become difficult to figure out how you separate that out in order to cover the portions of it that relate to public sector entities under FOIPPA when you've got all these other players in that single corporation. There are also entities that have business opportunities that have been bequeathed to them. Do you require them to be covered under FOIPPA when the majority of private business entities would be covered under PIPA? Then you've got an unlevel playing ground.

It's been very difficult to come up with criteria for what we would mean by a corporation and what would be the basis of what they would be covered on. Do you have so many of their people appointed to a board? Well, when you're looking at one that's got all those entities, you may not have any appointed to a board or you could have a few appointed to a board, but you're still bringing in all of these other parties.

There are a lot of complexities in there that we've been trying to sort through and think through, but we haven't come up with a magical solution yet that satisfies that. Any help would be beneficial in trying to set criteria for what and who would be covered.

D. Routley (Deputy Chair): Supplemental to that, previous recommendations have indicated that their recommendation would be to include subsidiary bodies wholly owned or controlled by a public body.

Do you imagine that thresholds could be established, like a percentage of ownership or number of persons appointed to a board, that could qualify a corporation under FOIPPA?

S. Plater: You could. What we've been trying to do is look at different criteria. We've asked universities, for example, for ideas around criteria. We've been trying to apply those across the different examples we've been given. We're still working through that. We still haven't come up with, as I said, a magical set of criteria that's going to be useful for coverage.

D. Routley (Deputy Chair): Would it be helpful for this committee to suggest such?

S. Plater: Yes, it would be.

D. McRae (Chair): Actually, I was going to ask a question as well, but I'll also make a comment.

[1115]

It might be seen with a little skepticism if universities were to make some suggestions how to better deal with third-party business ventures, since at this committee we've had a number of presentations by individuals and groups saying they have concerns over that area. That being said, best practice would be, I hope, recognized as best practice and something we could embrace.

S. Plater: Can I respond? One of the reasons we went to universities and asked that question is that the people who practice in the universities in the area of privacy have come from multiple different entities, including the commissioner's office, other types of the broader public sector, municipalities that are already covered for their corporations, etc. We thought they may have a wealth of ideas that we could take and at least throw into the hopper and think about.

D. McRae (Chair): Fair enough. My one question, though. We've had some presentations — in fact, we just had one this morning from Nelson — talking about proactive disclosure. I think you mentioned earlier there could be 8,000 to 10,000 FOI requests a year, and at some cost. Now, some are very simple. Will there be recommendations, from your final report, as to what areas we could actually address in proactive disclosure and make it a little easier for the ministries to deal with the more robust FOI requests?

B. Hughes: I did mention, in my speaking notes, one area where if we could change legislation to allow us to redact personal information from documents before we proactively disclose them, that is something that we think would be helpful.

D. McRae (Chair): Thank you very much. We'll keep going, then.

D. Eby: In follow-up on this wholly-owned-subsidiary issue, I'm surprised that you're seeking advice from this committee about how to implement this. I note in the Privacy Commissioner's submission — which we're going to be seeing following yours, and I recommend it to you — she notes: "In June 2014 and October 2011, I wrote to the relevant ministers to ask that an amendment be drafted to FIPPA to ensure that these entities were all public bodies that were covered by FIPPA."

Since October 2011, or perhaps since June 2014, you haven't been able to figure out a way to get wholly-owned subsidiaries under the Freedom of Information Act, any way to draft legislation to bring them underneath? If you haven't, if that's the case, have you advised the commissioner of your difficulty around this

and asked for suggestions about how to implement her recommendation?

It seems to me that this has been going on for a long time. This committee has heard from six or seven witnesses that this is a serious issue. We're going to hear from the commissioner, it seems, on it as well. I find it surprising that there are no records on this request.

B. Hughes: I'm not sure I understand your last comment that there are no records.

D. Eby: How can it be that since October 2011 this has been an issue — a huge issue for the public — in front of this committee for multiple years, yet this ministry has no idea about how to implement that recommendation and is, in fact, seeking recommendations from elected officials about how to do that?

B. Hughes: Yes, you're correct that this has been something that has been on our to-do list for a number of years. There have been conversations with the different entities, as Sharon mentioned. It is a very complex issue, and it is one of the many, many things that we are working on. Yes, we do have ongoing conversation with the commissioner's office. We know that this is something people are interested in. It is something on our minds.

D. Eby: I guess, maybe more pointedly, what I'm asking is: if we respond to the many recommendations we've heard from the public to recommend to you that wholly-owned subsidiaries be included under FOIPPA, how does this committee ensure that the response from the ministry isn't: "Well, this is quite complicated. We don't understand how to do it, so we're not going to do it"? Clearly, this is a significant concern of the public, and it's certainly a concern of mine on the committee. I don't know whether it's shared by other committee members. But it would be my hope that if we recommended that, you would be able to do that.

B. Hughes: Well, as with all the recommendations, we will take them under advisement and look at how we can action them.

K. Corrigan: I wanted to ask a question that I'm also going to ask of the Privacy Commissioner with regard to the submission that we've received from that office.

[1120]

I believe you were talking — certainly, the category was in there — about mandatory notifications when there's a breach. The recommendation made by the Privacy Commissioner is that if there is a data breach, they need to be notified of that and that if there are individuals that could be involved in a negative way, they should also be informed. But I'm wondering whether or not there is agreement that, in the public interest, there need to be requirements that there be public information about those kinds of data breaches. I'm just wondering if you have any comment on that.

Maybe I'll just add my last question, which was with regard to the drafting of amendments with regard to data linking. Just confirm that it is intended that there will be legislation and an amendment which will provide that the data-linking provisions which are too narrow will mean that if there is either one of the two groups involved…. It'll fix that loophole, basically. You know the loophole I'm talking about. Is that what you're saying?

B. Hughes: Yes. On the draft amendment to the data-linking provision, we have worked with the commissioner's office to come up with language and process that will address that issue.

With regard to the privacy breaches, generally, Sharon, if I can have you speak to the details around that.

S. Plater: The majority of privacy breaches that government gets or investigates are administrative. You have a very high percentage that are double-stuffed envelopes or a fax that's gone missing or a letter that's been sent to an address that's no longer in play. I think it would be important to think about whether those are in the public interest to notify the public about.

The other thing that we get as a percentage of the remaining breaches…. A fairly significant proportion of those relate to individuals. So you would have…. It's a child-in-care file, or it may be somebody in an adoption record. It could be somebody in a criminal file.

It's very much related to their particular circumstances, so again you'd really have to consider the privacy issues related to that when you consider public notification. I think there are a number of factors that you'd have to look at there and weigh as to whether it would benefit the public with such notification.

D. McRae (Chair): Just a reminder: we have about eight minutes to go. So, hoping that everybody gets their questions and we keep them brief.

D. Routley (Deputy Chair): I have two concerns about the failure to meet the test of the act on the part of a number of public bodies, ministries and the Premier's office. The commissioner's report points to the failure to meet the "duty to assist" requirement under the act and, in fact, describes it as a negligence under the act, in the Premier's office and other examinations the commissioner has made.

Since that has a very serious overtone to it, what steps are being taken by the ministry to ensure that ministries and public bodies are in fact meeting their requirement under a duty to assist applicants?

Then, also on the privacy-breach side of it, we saw the massive privacy breach — an unencrypted hard drive

that was lost. It was such an obvious failure to meet the test of privacy protection, any basic expectation. It's almost impossible to believe that that much personal information of British Columbians could be stored in such an irresponsible way.

What can the ministry do to encourage people working within the bureaucracy to recognize their responsibility to adequately protect privacy? I don't know where to start, even.

[1125]

B. Hughes: With regard to the duty to assist, I would add that both in the overall FOIPPA training that we do, as well as the specific training that's done by the information access operations, we have increased the training material and discussion around a duty to assist.

Wes didn't mention it in his last response, but where we…. There are a couple of things. When a request comes in and we don't believe the applicant is asking the right office for the records that they are looking for, we will work with the applicant to ensure that we help them figure out where the records may be that are responsive to the request.

Also, when we do receive a response back that there are no responsive records, staff do follow back up with the public body to ensure that…. They may not have records themselves, but do they know of other people within their organization that may have those records? So it's encouraging them to ensure that they have done a broader scan within the organization or other organizations that may have those records. And we will refer those requests.

So there is work being done to ensure people understand clearly their duty to assist in terms of responding to applicants' requests and that they think about it more broadly than just the request coming to their own office or them individually as to whether or not there are records that may be responsive somewhere else.

With regard to the privacy breach with the Ministry of Education, there is an investigation that is currently underway, both by my office and the Office of the Information and Privacy Commissioner, looking at how that occurred. But not waiting for the results of that investigation, we have increased our connection with the ministries to ensure that those ministry privacy officers and those ministry security officers are ensuring that staff within their ministries understand the policies that are in place, which do not allow for the storage of personal information on unencrypted devices.

That particular hard drive — it was 2011 when that information was put on there. There has been a significant amount of work since then to ensure that staff understand their obligations and ensure that they are using the appropriate technologies to store personal information.

The privacy management and accountability policy that I spoke to earlier and this community of practice that is in place — again, raising the awareness and also the understanding of the policies around protection of personal information. We have also hired Deloitte to assist us, particularly around the practices in the Ministry of Education with regard to the security of personal information, as well as working with us to develop a compliance review process that we will be carrying out in every ministry to be able to do a review to ensure that ministries are aware and are complying with our security and privacy policies.

D. Eby: I did want to ask a question. We had a couple of witnesses here on section 30.1 on storing data abroad as opposed to here in Canada. I'm certainly relieved to hear your interest in maintaining the critical aspects of that.

What I was curious about was the stuff that seems to have been caught that's more on the periphery. For example, we heard from — I think it was — Coastal Health about an employee satisfaction survey that they couldn't run through SurveyMonkey. We heard about the research universities having trouble with managing international student records or with their overseas campuses and so on. Has there been any discussion about how we maintain the critical piece of 30.1, which is making sure that U.S. intelligence doesn't get to just leaf through B.C. resident information but make sure that innocuous data potentially…? I don't know. Is there a way to address the potentially innocuous data without throwing the baby out with the bathwater here?

B. Hughes: We work with not just core ministries but the broader public sector when they are challenged by those provisions of the act in terms of meeting their business requirements.

[1130]

What we help them do is identify other options that may be available to them and also identify what they can do to see if they are able to utilize those technologies, either through development of their privacy impact assessments, making sure that they understand what those threats are and what might be in place in order to assist them with using the technology — things like tokenization — to be able to do that. So we do help ministries and the broader public sector to see if there are avenues to be able to take advantage of the technology while still being within FOIPPA.

Sharon, you probably have some more specific examples, because the folks are usually calling your office.

S. Plater: I just wanted to mention that because we work with all ministries and the broader public sector, we are aware of some tweaks that need to be made to the legislation in that area.

For example, you can get ministries where the only information that's leaving the country would be the name of the employee, where they're working — the physical

address — and their phone number. That's it. But because it's not being used to contact them — it may be being used for some other reason within the system development — that can't go outside of the country.

We're aware of pieces like that that make no sense whatsoever. Like you said, it's not sensitive data. They need to be addressed in legislative amendments. So we do have those on our radar.

Some organizations — if they have a very small, targeted change — could approach government about the possibility of a ministerial order. That's another option that's available within the legislation.

Oftentimes what will happen is an organization will come forward and say: "We want all of our material exempt. We want our e-mail, our SharePoint, all of our systems exempt." Well, that's not an appropriate move. There are many choices they could make — such as getting consent from individuals in order to share their information across borders, etc. — that are available already in the legislation. But if there is a small, targeted change that they can't accomplish any other way, then there is that option of a ministerial order.

D. McRae (Chair): Thank you very much for coming and joining us today. Thank you, Bette-Jo, Sharon and Wes. We appreciate it. We appreciate the presentation. We look forward to your report.

I'd like to welcome the Office of the Information and Privacy Commissioner of British Columbia today. Obviously, I'll let them introduce themselves, but we know them all.

Before they say anything, I'd like to say thank you very much. Deputy Chair Routley and myself were able to attend the conference. Your staff worked very hard, I know, last week. It was an amazing group of academics, private sector, lawyers, individuals with great expertise, including former Premiers, who came and shared their thoughts about privacy and freedom of information. So thank you, again, for doing that, not just for ourselves who attended but for all the attendees and for British Columbia, for coming together there.

[1135]

Most of all, my daughter Chloe wanted to say thank you for the little leather giveaway book at the end of it. She quickly took that from me when I got home and has been doodling in it ever since. She's six, and her pictures are outstanding.

That being said, could I turn the proceedings over to yourselves. Like we just had, we'll do a half-hour presentation and then a half hour for questions. The floor is yours.

E. Denham: Thank you very much. Thank you for your kind words about our conference last week. I hope that we are not the cause of the privacy bug that seems to have invaded you and Bette-Jo.

Hon. Chair, vice-Chair and members of the committee, I'm very pleased to be here today. With me is Michael McEvoy, who is our deputy commissioner, and my colleagues who have joined us, behind us.

You will have received a detailed written submission from my office. In that submission, we make 20 recommendations for legislative change, including a duty to document, including oversight and sanctions for destruction of records, mandatory breach notification and stronger privacy management requirements that will raise the bar for personal information protection in British Columbia.

I'd like to spend about the next 25 minutes talking about these key recommendations and then be prepared to answer any questions put to me by the committee.

My slide deck is quite simple, so there are no cartoons. There are no illustrations, but it might help guide you through my presentation.

Having reviewed the written submissions and following the transcripts of individuals who have appeared as witnesses before the committee in the past few weeks, I'm really heartened by the level of public engagement in the work of this committee. It's clear to me that British Columbians take a real interest in their information rights.

I'd like to start by talking about those information rights and, in particular, the duty to document. As committee members will know, on October 22, 2015, I released an investigation report called *Access Denied*. In it, I examined FOI responses within the B.C. government and made a number of recommendations for change.

Two of my recommendations have been referred to the committee for study by the minister responsible. The first is a duty to document, which is a positive duty for public servants to create full and accurate records.

The second area for study is oversight of records destruction and penalties for non-compliance. I thought it would be helpful to talk about why I think these legislative changes are needed and what they would look like in practice.

One of the main messages in my recent investigation report and in previous reports by my office is that access-to-information rights can only exist when public bodies create and keep records of the key actions they take and decisions they make.

I believe the duty to document is a critical element of good records management, which in turn, supports good government. This is especially the case in a world dominated by digital communications.

Some documentation is obviously taking place now. But if one were to take a snapshot today, it would be an incomplete picture of the what and the why of government decision-making.

The government's new Information Management Act defines and sets out the mechanisms for retaining government information, but it leaves unaddressed the need

to create that information in the first instance. Citizens might wonder how it is that any government can operate without creating information about its major actions and decisions.

How would an auditor come to understand the underlying basis or rationale for financial transactions if there is no written documentation? How would a lawyer, defending or initiating legal action on behalf of government, find the relevant evidence? In a democracy, how does the public hold its government accountable if citizens have no way of knowing how decisions were reached?

[1140]

Yet, increasingly, access-to-information requests are met with replies of "no responsive records," a phenomenon reflective of oral government, where some public officials do not write anything down.

A recent review into the firings at the Ministry of Health was hampered by what the lawyer conducting the review called a "dearth of documents," meaning that the records that would normally be available in a situation where discipline is being contemplated simply did not appear to exist.

A duty to document would ensure that there is a lasting record. The reality is that people's memories aren't perfect. Civil servants retire, or they move on to new opportunities. The bits and bites of information that aren't being documented are essential to understanding and following through on the important decisions being made.

After the release of my most recent report, there's been considerable public discussion about the duty to document. And there's some spirited debate about whether such a duty would be helpful or whether it would be harmful.

Those who oppose a duty to document typically cite two concerns. The first is that it would be just too cumbersome, forcing government officials to document every idea, every discussion, every meeting regardless of its import. But this isn't what my definition of a duty to document entails.

A duty to document does not necessarily require the production of more records. Rather, it requires the deliberate production and retention of records about specific mandated activities. In jurisdictions such as Queensland, Australia, where the duty to document is legislated, public bodies determine what functions and what activities they are responsible for and, therefore, what records they should create. Records that are created are those that support a public body's purpose, its operational needs, its statutory responsibilities. This brings clarity to the process of determining when a record needs to be created or should otherwise exist.

The second concern about a duty to document is that the disclosure of government's inner workings will chill the decision-making processes that are so vital to good government. Public servants, it's been argued, will be less willing to express frank views, including difficult truths that politicians may not want to hear, for fear they will be misunderstood if these views are publicly exposed.

However, our existing access-to-information law already takes into account this concern in the advice and recommendations exception under FIPPA. Certain kinds of behind-the-scenes discussions are not subject to disclosure, thus allowing for frank discussions. It does not follow that a duty to document will result in a duty to disclose.

What does a duty to document look like in practice? In thinking specifically about the B.C. context, I believe the duty should encompass three requirements.

First, it should be expressly written into FIPPA. This would ensure that the duty exists to all public bodies, not just core government, as is the case under the Information Management Act. This would also ensure that my office has oversight responsibility for the duty. I don't think that a duty to document in policy will suffice. I believe that recent events have made it evident that there needs to be a clear and unequivocal duty in law.

Second, the duty to document should be flexible enough to work for public bodies of different sizes and which are in different lines of business to establish practical and meaningful categories of records that need to be created. Consideration has to be given to business needs, accountability requirements and community expectations.

[1145]

For example, if a public body is making a decision to embark on a new program, staff would be required to document or record the decision and the basis of the decision to implement the new program. A social services agency would be required to document a decision around granting a benefit to an individual. A contract manager would need to document how a contractor's qualifications and services were scored in case they were challenged.

Third, there needs to be robust and independent oversight of the duty to document. Another issue explored in my investigation report and referred to this committee for study is oversight over the destruction of records.

This is an issue of public concern in British Columbia and elsewhere in Canada. We have an oversight gap in our laws. FIPPA provides very minimal oversight of the destruction of records and only in cases where a person obstructs a public body's response to an access request by destroying records. It's a very narrow piece.

The Information Management Act determines a schedule for the destruction of records by core government but not for the broader public sector. This means that if documents are improperly disposed of outside of the FOI process, there is no mechanism for investigation or review.

In Alberta, the Information and Privacy Commissioner has the power to investigate compliance with rules in provincial statutes or of local public bodies on the destruction of records. The Alberta statute establishes the unauthorized destruction of records as an offence.

My recommendation brings the Alberta model to B.C., with my office having the power to investigate allegations around the destruction of records under any B.C. statute and oversight over records destruction that's in contravention of rules or bylaws of local public bodies. This oversight should also be supported by new, complementary offences and penalties under the act. I'm going to speak more about penalties and sanctions later in the presentation.

I would like to turn now to some of the key recommendations that I'm making specific to the protection of privacy. My recommendations, if adopted, will raise the bar to ensure that public bodies properly manage personal information of British Columbians in an accountable way.

I know we've already talked about this, but I'd like to start with my recommendation for mandatory breach reporting.

We trust public bodies with our most sensitive personal information — health records, tax records, financial information, and the list goes on — and turning over much of this information to government is not optional. We need health care. We enrol our children in school.

When we need the services of government, we have no choice but to hand over our sensitive personal information. But it seems that every week the public learns about a new data breach involving lost or stolen laptops or mobile devices; misdirected e-mails containing sensitive data; or employees snooping in electronic health records.

Privacy breaches carry a human cost. They put individuals at risk of identity theft, serious reputational harm — not to mention the loss of confidence of the public in government agencies.

Breach reporting in British Columbia is currently voluntary. My office only receives reports in 1 percent of cases of data breaches. A voluntary regime means that there's no clear threshold for reporting to my office, no consistency in when breaches are reported to affected individuals. Therefore, it's incomplete.

Mandatory breach notification would give citizens an opportunity to be made aware of these significant breaches and take steps to mitigate them. There should also be a legal requirement to report significant breaches to my office so that our staff can assist public bodies to address the breach, address its root cause and help to prevent future occurrences.

[1150]

B.C. would not be charting new waters with such a provision. Newfoundland and Labrador and the territory of Nunavut have such provisions in place, and seven of Canada's provinces have mandatory breach reporting requirements in their health information statutes. The federal government addresses breach reporting through policy.

In November of last year, I made a presentation to the special committee reviewing PIPA, the Personal Information Protection Act. As part of those consultations, I outlined why mandatory breach reporting would be an important addition to the private sector legislation. The committee agreed and recommended in their final report that PIPA be amended to require organizations to notify the commissioner and affected individuals in the case of a significant breach. There should not be a lower standard for the protection of privacy in the public sector.

Privacy breach reporting is only one part of an overall privacy management program. Just as public bodies must have sound financial management practices and frameworks, they must also take a comprehensive approach to privacy.

Canada's privacy commissioners have issued detailed, scalable, practical guidance that provides private and public sector organizations with a road map to implementing sound privacy management. This committee has an opportunity to take this work to its next logical step: an express legal requirement spelling out what public bodies need to do in order to effectively protect the privacy of individuals.

The special committee reviewing PIPA made this recommendation for the private sector. While there are some differences, in my view, the obligation should be harmonized between these two laws to provide for the same legal privacy requirements, including appointing somebody to be in charge of privacy within a public body, staff training — not required right now; it should be in law — privacy policies and privacy breach response plans.

Privacy management programs do not prevent every breach, but they go a long way to providing proactive tools to mitigate privacy incidents and also, really importantly, build trust with citizens. We've begun to see privacy management implemented on a policy basis. We heard that the government of British Columbia has implemented a policy control privacy management program. But the broader public sector — education bodies, health authorities, municipal governments, universities and Crowns — should also be implementing controls to effectively protect personal information.

Of course, all of the recommendations that I've been talking about here and in my written submission require robust and independent oversight in order to be effective.

Before I move on to our Q and A, I received two written questions from the committee that I would like to respond to.

The first concerns health information and how it should be dealt with in this review. Unlike most other provinces, British Columbia does not have sector-specific, stand-alone health information legislation. Depending on the provider of the health service, personal health information may be subject to FIPPA, it may be subject to PIPA, or it may be subject to the E-Health legislation.

I've long said that I believe British Columbians would be better served with a single set of rules that facilitates the flow of information between the public and the private health providers — also to ensure robust protection for patient information and also, really importantly, to

establish a framework for vital public interest research. It's not expected that B.C. will adopt a stand-alone law for personal health information any time soon.

While this committee is tasked with reviewing FIPPA, there are a number of recommendations that I'm making that are particularly important for strengthening the protection of personal health information. I believe breach notification requirements proposed would be of great importance to the health sector. Much of the information in the health sector is stored in electronic form in large databases. That means that the risks and the potential harms of privacy breaches are greater than they were in the days of paper-based records.

[1155]

Similarly, I believe that my recommendation around data linking is also important to the health sector. Currently there is a carve-out for data-linking rules for the health sector. I believe the rules should be applied to personal health information, which would make them subject to transparency and review, and my recommendation for new offences and higher penalties will match those in other Canadian jurisdictions.

There have also been numerous reports of employees snooping in electronic health records in B.C. and in Canada in the last year. While this is not a problem that's exclusive to health information, it has proven to be a particular problem in that sector.

Finally, I would like to answer a question I received from the committee about a framework for sanctions and penalties. FIPPA currently authorizes penalties for two types of offences. General offences carry penalties for individuals up to $5,000, while privacy protection offences for individuals carry penalties of up to $2,000.

These penalties are among the lowest in the country. Other provinces have penalties ranging from $10,000 up to $50,000 per offence. Ontario has passed a bill that will increase penalties to $100,000 for individuals. I think B.C. needs to come in line with these other jurisdictions and deter would-be offenders, so I'm recommending penalties for general and privacy offences committed by individuals under FIPPA to be raised to $50,000.

I also recommend two new offences: the unauthorized and wilful destruction of records and for unauthorized access and use of personal information — in other words, the snooping offence.

I just want to leave you with a quick postscript. While this is not written in my submission, I believe the Legislature should review FIPPA more frequently than every six years. Given the fast pace of technological change and the myriad of access and privacy issues that continue to wash ashore in British Columbia, I believe that a review every three to four years would allow legislators to ensure that information rights are protected on an ongoing basis. I leave that for the committee's consideration.

Thank you very much for your attention this morning, and I am pleased to take any questions.

D. McRae (Chair): Perfect. Thank you very much. I'm sure we will have some questions.

K. Corrigan: I want to thank your office for the work that you do on an ongoing basis, including the report that you referenced from a few months ago. I wanted to try to home in a little bit more on where the line is on what types of documents should be preserved. One of the questions is….

On page 6 of your report, talking about the Information Management Act requirements, it says that information that should be kept, essentially, is: "(b) information that documents a decision by a government body respecting a course of action that directly affects a person or the operations of the government…" and then, in addition to, "(c) information that documents or supports the government body's organization, policies, procedures, transactions or operations."

I know that when we were raising issues in the House about the report that was done — *Access Denied* — one of the responses of government that came back fairly regularly was: "Well, we don't have to preserve drafts. We just have to preserve the decision, and we did that."

Where is the line? Often it turns out that some of the damning information deals not with the decision or even the points up to it but, for example, e-mails that we find that go to the credibility of individuals or of government. It doesn't really have to do with the decision but rather credibility and other issues about the character of government.

Can you give me a bit of an outline of where you think that line is — of what should be preserved and what doesn't need to be preserved? It's very complicated, and I'm asking you to make very general comments, but….

[1200]

E. Denham: I think there's a lot of expertise in the records management field that can help answer those questions. Certainly, the definitions that I am quoting in my report from the Information Management Act are a start. They're a start to get us thinking about what records, in relation to the context of a specific program or a specific decision-maker in a public body, need to be retained.

You know, I look to the expertise of someone like Laura Millar, who presented to the committee. Her point was that once you figure out what evidence needs to be preserved, depending on the mandate of the public body…. Obviously, B.C. Ferries is not going to be creating the same kind of evidence of its decision-making as the Ministry of Children and Family. These are different business lines. But once you figure out what kinds of records actually matter to your function and your business line, then the transitory question is less troubling. That's one way of thinking about it.

I do think that what is needed here is a culture of proper creation and proper retention of important records.

Training is really critical. Leadership and the culture of leadership is really important.

Then you asked me a question about drafts. I'm going to say it depends. There are policies and guidelines around what is a record and what is a transitory record in terms of drafts.

I would say that a draft of a cabinet submission is a record because it's going to change along the way. I would say that the draft of legislation is a record and not transitory because the changes that were made along the way are reflective of decision-making. A draft of a briefing note that one of my staff writes to me may not be a record and may indeed be transitory.

It's contextual. It needs clear direction. It needs training. But I think we already have a lot of tools that we can use from various jurisdictions to be able to clarify this issue.

D. Routley (Deputy Chair): I have quite a number of questions. I'll just stick to….

D. McRae (Chair): How about you do a couple. Then we'll keep moving around, and I'll come back to you.

D. Routley (Deputy Chair): I'll do a couple, and we'll see what happens.

Thank you for the presentation, of course. In your report, you referred to an indication that the practices you identified as problematic were probably systemic, but your investigation was not broad enough to make that assertion directly. What would it take in order to review government to the point where you could satisfy yourself that it is or is not systemic?

E. Denham: You're correct that the statement that I made in my report is this was not an audit of government's duty to assist. We had three complaints, and we followed those complaints. We did not go in and look at various files that the government had on "no responsive records" or problems in duty to assist. We did not do that.

Committee members may be interested to know that I am doing such an audit of the city of Vancouver in terms of their duty to assist applicants. In that review, I would say that's going to be more of a systemic, broad review of their practices. We don't have the resources in our office to do a broad, systematic review of duty to assist within the provincial government.

I'm hopeful that with the government's commitments to adopt and accept the recommendations in my report, with the expert advice of David Loukidelis on things like training and policy…. By the way, I don't think that his terms of reference cover making recommendations on legislative reform. I think that's up to this committee. But I look forward to his report to the government.

[1205]

Then instead of doing a timeliness report, which I have done with regards to FOI in previous years, I will consider going back and doing some spot audits in ministries where we see some patterns of problems. That's the extent that our resources will allow.

D. Routley (Deputy Chair): We've heard from several public bodies and organizations, companies, in fact, that have come forward and recommended that we relax the protections under section 30.1 that prohibit storage of personal information outside of Canada. I'm very concerned about that, particularly since the convention that we attended, the Chair and I, last week that you hosted.

It was really an eye-opener when Lisa Austin from the University of Toronto shared her work. She said that, in fact, if we share our information in the United States, we are not protected, as non-resident aliens, under the Fourth Amendment of the constitution.

In any case, Charter protections in Canada of privacy are more stringent and strong, but we would also lose those protections, because any search would be a search for information outside of Canada, so a Canadian authority would not be bound by our Charter rights. That's a huge concern.

We've heard today from a contributor to this committee that perhaps our right to maintain section 30.1 is not threatened by trade agreements, TPP in particular. But if we were to relax it, I would suggest that it would be very difficult to turn back and increase again, given the restrictions that are there. Can you give this committee any recommendation as to what we should do in terms of these petitions?

E. Denham: I was hoping I wouldn't get the difficult 30.1 question. But like you, I was listening intently at the panel on data localization and data sovereignty last week in Vancouver and Lisa Austin's work, which basically says jurisdiction still matters. So data localization is an important tool. The Maple Leaf constitutional protection does not follow our data when it leaves the country, whether it goes to the U.S. and it's in the hands of a cloud provider or elsewhere.

Essentially, the concerns that led the Legislature to make the data localization provisions remain unchanged. When I talk to British Columbians, they tell me that their privacy is really important to them and that they don't want their sensitive personal information to be compelled to be produced under a foreign law. They want the protection of our Canadian constitution. They want the protection of our privacy laws, which they lose once the data crosses the border.

When I talk to British Columbians, they don't know a lot about the details of their privacy protection under our FIPPA or under our PIPA. But what they do know about the Freedom of Information and Protection of Privacy Act is that their data can't be transferred outside of Canada ex-

cept in those circumstances where they give their consent. British Columbians do know this about our law.

To take that away, to repeal that requirement, I think the legislators would have to think about what to put in place to protect data in the long term. I don't know what that is, especially.... As we heard from my government colleagues, the invalidation of the safe harbour agreement, the European Court of Justice, means that there are questions around the bulk collection of data and the lack of protection for foreign nationals, for their information in the U.S.

I don't see those concerns abating. I don't see any kind of a rollback of those provisions where information can be collected in secret under the Freedom Act, which amended the Patriot Act. I don't see any changes there.

[1210]

That said, we also meet with the education sector, the health sector. We hear their concerns and the difficulties and frustrations that they may feel. However, I think the landscape has changed. I think you can see players like Microsoft and Adobe that are setting up Canadian solutions.

We have surveyed companies in Canada that public bodies could use. So I see some easing of those difficulties. Are they going to go away completely? No, but we do have amendments in our law that allow for consensual disclosure, that allow for a ministerial order when something is in the public interest and needs to be shipped across the border.

I'm not hearing anything that convinces me that we need to roll back those provisions. You will have noticed that I didn't make a recommendation for change in my submission.

D. Routley (Deputy Chair): I just want to express my agreement with that and my concern that British Columbians will answer at a very high percentage that personal privacy protection is a highly salient issue for them but not really understand the architecture of what the law is or what mechanisms are there to protect them.

I think it puts an even higher onus on members of this committee and on government to be responsible gatekeepers of that privacy, even though people might, without much concern, click "I accept" on a Facebook privacy notification. We have a much higher duty, and I'm concerned that this push for expediency around 30.1 will be undermining all of that.

I thank you for your submission.

S. Sullivan: I listened to you about the duty to document. I think about my own situation. Every couple of years I make this goal as a new year's resolution that I'm going to document things that I do, and I never do it. Or sometimes I do, but I write very incompletely, and when I look back, I say: "That really doesn't represent what happened." But it's my attempt.

So I do worry about old guys like me — you know, trying to get us to document everything we do, especially if we feel that whatever we write, we'll be judged on. If they're not complete, you'd really.... If you think there's going to be a court case or something about this, then you certainly want to make it complete. There are certain people that just like doing things and not writing things up. It's kind of a personality issue.

I just wonder about the training that would be required and how effective training could be for some people if it's just not a habit for them to write everything down.

E. Denham: Just to be clear, I'm not suggesting that a duty to document means that everything needs to be written down. Again, it's selective. If there's an important decision that's made at a meeting, then it needs to be recorded — after the meeting, as a note to file, in the minutes of a meeting. If it's important and it's related to a mandate, then I think there needs to be a record.

In the olden days before digital communications, there would probably be a stenographer that was making a record. That person would go and file that, and that decision would be available. But now everybody is a records manager, and everybody is creating or not creating records and filing them who knows where.

We've got a records management challenge that's not just unique to B.C.; it's a challenge everywhere. So we have to come to terms with the new technologies, and we have to train people on what's important to write down and who's going to be the office of record, to keep that record so that it's available for just good practice and good government. It's not all about FOI.

I'm just saying there needs to be training. There needs to be expertise, and there are some experts within government. They're in a centralized unit. Maybe what needs to happen is have those records officers available throughout the various public bodies. But it can be done.

[1215]

D. Eby: With respect to your recommendations around penalties in the hypothetical situation of a senior public servant destroying records and instructing subordinates to destroy records inappropriately, would the fine be levied against that individual or against the ministry? Is there a possibility that a department, for example, could be fined?

E. Denham: Our recommendations around penalties and sanctions for the unauthorized destruction of records are to the individual. Again, I think if individuals were not trained, were not made aware of policies, etc., then it could be an issue for the ministry or the public body.

But once people have been made aware of what their obligations are under statute and policy and an individual decides to destroy records, that's an illegal act and it should be a penalty against an individual.

I have some reservations about fining public bodies under the Freedom of Information and Protection of Privacy Act, because really, at the end of the day, you're hitting the taxpayer. I don't know how workable fining public bodies for the action of an individual is when that individual was warned, trained and aware of policies. So these are fines against individuals.

There have been fines and sanctions and penalties against individuals in other jurisdictions for improperly accessing personal information and destroying records.

D. Eby: We heard from the ministry that the issue of wholly owned subsidiaries is a very difficult one and, in fact, for years they've struggled with it and still have no idea how to deal with this. In fact, they asked this committee for help. As enthusiastic as I am to help, I don't feel qualified to do it.

Can you provide this committee with some assistance in understanding the legislative provision that would be needed to bring wholly owned subsidiaries — for example, in the case of school boards' own incorporations, universities or so on — under the provisions of FOIPPA? We heard from a number of witnesses that this was a significant priority.

E. Denham: I do think it's a significant issue. We've certainly written to ministers over time and talked about this in other FIPPA reviews. The bottom line is when public resources are used to operate a subsidiary corporation, then that subsidiary corporation should be subject to the accountability and transparency requirements in FOI and also follow privacy rules.

I was aware that there were stakeholder consultations going on, that the ministry was talking to various public bodies and third parties. But I was not aware of the difficulties that they were having until I heard this presentation today.

Without giving prescriptive, legislative language as to what the fix is, I'm certainly able and willing to work with government to come up with that wording. I have made a suggestion in my submission, but I also understand that there's a lot of dialogue going on about the percentage of ownership, etc. The other thing that I would do is look to other jurisdictions for how they've solved this problem.

D. Eby: My fear is that we'll make a recommendation and it won't be implemented because of concerns that it's too difficult, so any assistance you could provide in that regard would be very welcome.

The last question for this round. Mr. Loukidelis has been asked to do a report to assist the ministry in implementing your recommendations. Can you advise this committee what role, if any, you have in Mr. Loukidelis's report? Will you be consulted? Should we seek to get a written submission or to get you to appear again after that report is out to help us get your feedback, or can we assume that your feedback is incorporated in that in some way?

E. Denham: I have not been approached by the government as to how I will be involved in Mr. Loukidelis's work. However, I would assume that I would be able to have access to his report before it's made public because the purpose of his review is to comply with the recommendations that we issued in this report.

I think it's important that our office feels that the work that he has done will assist the government in meeting the spirit and the letter of the recommendations. I would be interested in appearing before this committee again once that work is complete. Also, if there's anything else that our office can do as follow-up work from submissions that you receive at the end of January, we can provide comments or review opinions, if that's helpful.

[1220]

K. Corrigan: It's sort of off the main topics that you've been talking about. Page 31 of your submission says that FIPPA should set out a clear threshold at which a public body is required to correct personal information and that that threshold should be harmonized with the reasonable grounds threshold set out in PIPA.

I was wondering about whether you have in the past…. Maybe you've done a report on this, and I've missed it. Have you looked into…? I think you have, actually, looked into PRIME-BC before.

My concern is that there is something like…. I can't remember the last count. It was about 4½ million records of personal information about British Columbians in there — some of it duplicates, some of it old. We've certainly, as MLAs…. I know many of us have had people come and complain about the fact that it's affecting their ability to get work when you get a report from PRIME. This is a police database — inability to cross borders without really knowing why and so on.

Maybe you could just comment a little bit more about that and how this recommendation affects that.

E. Denham: There is a relationship. I'm going to ask Michael McEvoy to address it. We have looked at police information checks in the past. I think that's what you're remembering.

K. Corrigan: Yes.

M. McEvoy: Some of the concerns that you've raised we've heard directly with our office too.

The challenge with the legislation as it is now is it actually doesn't set out when public bodies are required to correct personal information. Ultimately, the remedy in the circumstance may only be that the record is annotated, even where it may clearly be that the information is incorrect. There's no obligation to do that.

The proposal, the recommendation, that we're making to the committee would at least set a threshold whereby the information would actually be corrected. It would set a standard whereby some of those very concerns that your constituents have raised and some of those concerns that have been raised with our office, I think, can be dealt with, we would say, in a more satisfactory way.

K. Corrigan: I have another question, another quick one. I wanted to ask a question about something that I asked of the ministry as well. It has to do with mandatory reporting of data breaches.

Your recommendation — and I think government agreed with it — is that yes, there should be a framework for mandatory circumstances when reporting of data breaches is mandatory; that if individuals are affected, they should be made aware; and, also, that there should be reporting to your office if a large number of individuals, perhaps, are affected.

My question before and my question to you as well is: have you thought about the importance of publicly reporting when it is fairly significant — adding a public reporting? Or would you think that it would be sufficient to simply say that it would be up to the Office of the Information and Privacy Commissioner to decide at what point a data breach was significant enough that it should be publicly reported?

I do understand the issues of privacy and mentioning names. I'm not suggesting that at all. I just think the very fact that there have been significant privacy breaches would be in the public interest, probably.

E. Denham: There are some jurisdictions, particularly in the United States, where significant data breaches must by publicly reported. I think of the state of California, for example. There is a requirement for at least private sector organizations to make public significant data breaches that reach a certain threshold.

In this model, if a large number of individuals are affected by a significant data breach and that report comes to our office, it's very likely that we would do a public report when it's a significant breach, such as the one that we were talking about with the Ministry of Education. The other point is that when there is mandatory notification to affected individuals, it's very likely that those affected individuals are going to make it public.

I'm not sure if the publication of significant privacy breaches is necessary to meet the policy intent of my recommendation, which is to focus more resources on proper data security.

[1225]

At the end of the day, what this is about is not "gotcha." It's not announcing it in the headline that there's been a breach. It's to focus attention and good care of our personal information. Knowing that breaches have to be reported to individuals and to the commissioner is really important.

D. McRae (Chair): Doug, you had withdrawn your question, or was it dealt with?

D. Routley (Deputy Chair): Actually, I will ask a question. Thank you, Chair.

The definition of a transitory document. There was work done around the time the original act was passed. Rob Botterell presented to the committee and brought that to my attention. Do you feel as though the definition adopted at that time, if you're familiar with it, is satisfactory today?

E. Denham: I think the definition could be tweaked. I think there's some work that needs to be done.

I think a more significant issue was the one that I was talking about earlier. Given that we have all these new forms of communication, we need to think about this. We need to train people and remind them about how the world is changing. What's government information that needs to be retained as evidence of decision-making? The rest of it — "Do you want to meet for lunch?" or "I've got to change the meeting to two o'clock" — is going to be a transitory record.

D. Routley (Deputy Chair): The act, being essentially technologically neutral, already accommodates everything we need to establish such a definition. We just need people to better understand the principles.

E. Denham: That's correct.

D. McRae (Chair): The next question goes to Sam, and then the final question will be to David.

S. Sullivan: We had a couple of presenters. One was on the high school yearbook, where their information couldn't be sent to the U.S. to get printing because it had the information about what they liked to do when they were in school or something like that. Also, some of the restrictions on sending the data out made the groups not able to access the latest technology for software and data manipulation.

I'm just wondering. Is there a certain test as to what risk the data really has by letting it out? The issue of the school yearbook was a good one. Maybe there's not a lot of risk of someone having something bad happen with that data out, since it's listed in public anyways.

E. Denham: I think the solution to the yearbook question is consent. Consent is a tool that can take care of that. If you think about the number of consent forms that parents have to sign for their kids in the context of attending school, I don't see why that can't be a solution. There are other solutions, such as ministerial orders. The minister could say that it's in the public interest that this information be disclosed outside of Canada.

Our provision is not risk-based. It says that personal information has to be stored and accessed within Canada, except consent, ministerial order, use of social media.

There are tools. Again, I haven't been persuaded that there aren't solutions to some of the challenges that public bodies are facing. I understand it's frustrating, but I think the whole world is grappling with this problem. I haven't heard that British Columbia's solution is out of date, specifically in the context of the European decision about safe harbour.

M. McEvoy: If I could just briefly add to that. The commissioner has said, myself and a number of other people who are actually behind me, on the task of engaging, particularly with the K-to-12 sector, where…. There are many opportunities to use some of the latest and greatest in technology to engage kids in learning, to look for solutions that allow for the use of that technology while still complying with section 30.1.

In a number of circumstances, I think, we've found a way to do that — not in all. It's not a completely magic bullet. We recognize some of those challenges and work carefully and methodically with members — again, as an example, with the K-to-12 community — to find some of those solutions and to allow kids to take advantage of some of the technology.

[1230]

D. Eby: The issue of resources of the OIPC has come up a couple of times. I note in particular that in your report *Access Denied*, there was a significant level of resources expended in technological expertise related to the metadata and so on.

Do you, under our existing legislation, feel that you have the tools necessary to access additional resources when you need them for major investigations, without compromising your existing obligations under the act?

Then the second is: I was hoping you could just provide a little clarification around "significant breach." What is a significant breach? For me, my data being breached would be significant. But is that what you mean — one person's data and so on?

E. Denham: I'm going to start with your second question. It was: what do you mean by a significant breach? There's a whole body of policy work and commentary and research around what a significant breach is. Forty-seven states in the U.S. have mandatory breach reporting laws; the European Union's new regulation — mandatory breach; the U.K., etc.

Really, it's a risk-based or a harm-based test. Is the disclosure of data reasonably expected to cause harm to the individual? That harm is not based on just financial harm. It could be reputational harm, etc. That would be a requirement to notify the individual and to report to our office, either where there is significant harm to the individual — expected significant harm — or to a large group of individuals.

There's a lot of research and policy around the determination of what a significant breach is. I can certainly provide more detail on that to the committee.

How could I forget about the resource question? I'm talking to some of your colleagues tomorrow. I'm making a presentation to the Finance and Government Services Committee with my ask for the budget next year.

I will tell you that we had to expend about $50,000 to bring in some expert resources and have legal counsel to assist us with the investigation in *Access Denied.* So we had forensic examination of metadata, etc. That was an extraordinary expense.

However, I'm finding that more and more of our investigations require the use of a forensic lab. We are looking more and more at digital technologies and investigating on the privacy side and on the access side.

The short answer to your question is: no, I don't have significant resources. The other problem we have is a large backlog of access-to-information appeals. Most files that come into our office have to sit in a queue for six months before they're assigned to an investigator, because we don't have enough resources to assign to those files. I can't give an investigator more than 35 files on their desk. There is a long wait for our services. I believe that's unacceptable to British Columbians.

D. McRae (Chair): Thank you very much. I'd like to thank the Office of the Information and Privacy Commissioner and all of the presenters today for their well-thought-out presentations, whether they were in person or via technology.

I'd also like to remind the people presenting today, those in the gallery and those watching at home that if they wish to make a submission in writing, they can do so up to January 29, 2016. I thank the committee members for their efforts today — and those who presented.

Thank you, and I adjourn this meeting.

The committee adjourned at 12:33 p.m.

Hansard Reporting Services

Director
Robert Sutherland

Manager of Reporting Services
Christine Fedoruk

Publishing Supervisor
Laurel Bernard

Editorial Team Leaders
Janet Brazier, Karol Morris, Robyn Swanson, Glenn Wigmore

Technical Operations Officers
Pamela Holmes, Dan Kerr, Yvonne Mendel

Indexers
Shannon Ash, Julie McClung, Robin Rohrmoser

Researchers
Liz Belsten, Mike Beninger, Mary Beth Hall, David Mattison

Editors
Kim Christie, Deirdre Gotto, Jane Grainger, Betsy Gray,
Iris Gray, Linda Guy, Barb Horricks, Bill Hrick, Jessica Hutchings,
Catherine Lang, Paula Lee, Donna McCloskey, Bob McIntosh,
Anne Maclean, Jill Milkert, Lind Miller, Erik Pedersen, Janet Pink,
Amy Reiswig, Murray Sinclair, Antoinette Warren,
Heather Warren, Arlene Wells, Kim Westad

Published by British Columbia Hansard Services,
and printed under the authority of the Speaker.

www.leg.bc.ca/cmt

Access to on-line versions of the report of proceedings (*Hansard*)
and webcasts of committee proceedings is available on the Internet.

Ministry of Finance

BRIEFING DOCUMENT

To:	Athana Mentzelopoulos Deputy Minister	**Date Requested:** **Date Required:**	March 23, 2016
Initiated by:	David Curtis ADM, Corporate Information and Records Management Office	**Date Prepared:**	April 4, 2016
Ministry Contact:	Sharon Plater	**Phone Number:** **Email:**	250 356-0322 Sharon.Plater@gov.bc.ca

350327

TITLE: Preparation for Deputy Minister's legal briefing on FOIPPA and other information management legislation.

PURPOSE:

(X) FOR INFORMATION

COMMENTS:

The Deputy Minister will receive a legal briefing on FOIPPA and other related information management legislation on April 8, 2016 from Kerri Sinclair, Legal Services Branch solicitor and an accompanying policy briefing from Sharon Plater, Executive Director of the Privacy Compliance and Training Branch (PCTB).

Executive Director approval: _____ ADM approval: _____

DATE PREPARED: March 23, 2016

TITLE: Preparation for Deputy Minister's legal briefing on FOIPPA and other information management legislation.

ISSUE: Deputy Minister to receive a legal briefing on FOIPPA and other information management legislation on April 8, 2016

BACKGROUND:

A legal briefing is scheduled to take place on April 8, 2016 for Deputy Minister of Finance, Athana Mentzelopoulos on the *Freedom of Information and Protection of Privacy Act* (FOIPPA), which was placed under the purview of the Minister of Finance in December 2015.

FOIPPA, British Columbia's public sector privacy legislation, was passed in June of 1992 and came into force for provincial government ministries in October 1993. FOIPPA governs the collection, use and disclosure of personal information by the public sector and applies to over 2,900 public bodies including ministries, local governments, schools, Crown corporations, hospitals, and municipal police forces.

As the Minister responsible for FOIPPA, the Minister of Finance has a number of duties and responsibilities under the Act. Many of these duties and obligations are delegated to the Privacy, Compliance and Training Branch, including: review of all ministries' privacy impact assessments, publication of the Personal Information Directory and development of directions respecting information sharing agreements and privacy impact assessments. There are, however, some duties which may fall to the Deputy Minister. These responsibilities include:

- receiving reports of foreign demands for disclosure of personal information;
- issuing ministerial orders to establish common or integrated programs or activities under the Act; and
- establishing categories of records that are to be made available to the public without a request for access.

- An overview of FOIPPA is attached as **Appendix 1**.

The Office of the Information and Privacy Commissioner (OIPC) provides independent oversight and enforcement of FOIPPA, as well as the *Personal Information Protection Act* (PIPA), British Columbia's private sector privacy legislation, which applies to over 380,000 private sector organizations including businesses, charities, associations, trade unions and trusts. An overview of PIPA is attached as **Appendix 2**.

Commissioner Elizabeth Denham is British Columbia's third Information and Privacy Commissioner and was appointed in May 2010 for a six year term. Her term is due to end on July 6, 2016 and she will not be seeking reappointment. Ms. Denham confirmed

this in a letter to the Minister of Finance, dated March 22, 2016, where she informed the Minister that she has accepted the position as the Information Commissioner for the United Kingdom.

Along with FOIPPA and PIPA, the new *Information Management Act* (IMA) is also under the purview of the Minister of Finance. The IMA, which will be brought into force this spring, replaces the *Document Disposal Act* as government's primary information management statute. An overview of the IMA is attached as **Appendix 3**.

DISCUSSION:

Section 80 of FOIPPA states that at least once every six years, a Special Committee of the Legislative Assembly must be appointed to undertake a comprehensive review of the Act. The most recent Special Committee was struck on May 27, 2015 and has received submissions during its public consultation period from government, the OIPC and other stakeholders. The Special Committee has until May 27, 2016 to submit a report of its review to the Legislative Assembly, which will include recommendations for changes to the Act.

As government awaits the Special Committee's report on FOIPPA, it is anticipated that recommendations will be made regarding the following issues, which were discussed by the Commissioner at length, during her submission:

Duty to Document

Commissioner Denham has recommended that government legislate a "duty to document" key decisions and actions. Though the Commissioner previously supported the inclusion of a "duty to document" in the IMA, she is now advocating for its addition to Part 2 of FOIPPA. The rationale for this shift is due in large part to the broader scope of FOIPPA (2900 public bodies) and its independent oversight provisions, which give the Commissioner her powers and authority. s.13

s.13

Subsidiary Corporations

A longstanding issue, which the 2010 Special Committee recommended be addressed, is the inclusion of subsidiary corporations of public bodies under FOIPPA. Corporations created or owned by ministries, Crowns, universities, school boards, health authorities, and other types of "local public bodies" are not currently under the scope of FOIPPA. The Commissioner has proposed that the definition of public body be broadened to include all boards, agencies, committees, commissions, panels and agencies in addition to corporations that are created or owned by a public body. s.13

s.13

Privacy Breach Notification and Privacy Management Programs

The Commissioner has also proposed amendments to FOIPPA that would make privacy breach notification and privacy management programs mandatory for all public bodies. Government currently provides monthly reports to the OIPC about each privacy incident investigated by government and reports all "serious" privacy breaches directly to the Commissioner. Government has also recently issued a corporate Privacy Management and Accountability Policy (PMAP). s.13

s.13

Oversight over the Unauthorized Destruction of Records

The Commissioner has recommended that FOIPPA be amended to give her office oversight over the unauthorized destruction of records as set out in any enactment in British Columbia, or any legal instrument that is used by a local public body, as well as the associated offences and penalties. s.13

s.13

s.13 The destruction of records is currently governed by the *Document Disposal Act* and going forward will be covered by the *Information Management Act*.

For a complete list of the Commissioners recommendations to the Special Committee please see **Appendix 4**.

Attachments

Questions and Answers

Ministry of Finance - FOIPPA Special Committee

DATA RESIDENCY

Q: Submissions from several stakeholder groups highlighted the limitations that the current data residency provisions in FOIPPA, specifically section 30.1, place on their operations. Does government plan to amend FOIPPA to address these concerns?

- Government will continue to monitor changes to privacy laws in other jurisdictions within Canada as well as abroad.
- The European Union is moving to bolster its data-residency provisions, with its proposed Data Protection Regulation, which will strictly regulate businesses who hold data within Europe as well as those outside of Europe who hold the personal information of EU citizens.
- While government is taking the recommendations provided by stakeholders under careful consideration, we must remain mindful of privacy trends in other jurisdictions. Shifting out of alignment with our international peers could have negative implications for BC in regards to trade.

SUBSIDIARY CORPORATIONS

Q: The issue of Subsidiary Corporations remains unaddressed by government. Submissions received by this Special Committee as well as past Committees have called for change. We would like to know if government has given any more consideration on this matter.

- Currently, corporations that are created or owned by "local government bodies" (which include municipalities and regional districts) are, by definition, already covered by FOIPPA.
- This is not the case however for corporations created or owned by ministries, crowns, universities, school boards, health authorities, and other types of "local public bodies". These corporations are not, by

definition, covered by the Act, nor are corporations that are partially owned or owned by more than one body.

s.13

"PUBLIC INTEREST" DISCLOSURE PROVISION

Q: How will government respond to the OIPC's new interpretation of the "public interest" provision? Will government amend section 25?

- In their July 2015 report regarding the review of the Mount Polley tailings pond failure, the OIPC found that section 25(1)(b) should not be interpreted to require an element of temporal urgency in order to require the disclosure of information that is clearly in the public interest.
- The ministry is currently working to determine how the OIPC's new interpretation of 25(1)(b) should be applied to records.
- The Commissioner has exercised her powers in adapting interpretation of this subsection and as such, no legislative change is required.

- Government will continue to bolster its training and awareness around the issue of section 25 compliance.
- Government has issued a guidance document, which was distributed through executive- and staff-level communication channels, and has emphasized section 25-specific content in regular FOIPPA training sessions.
- In moving towards making more proactive releases of information, section 25 is one mechanism that government will be looking at in order to make information available to the public.
- In addition to section 25, which is generally a broader notification to the public, limited public disclosure provisions under the disclosure provisions in section 33. This more limited disclosure provision is often used in instances such as a violent offender being released into a small community.

ACCESS FEES

Q: Fees for access requests was an issue raised by some of the stakeholders who presented to the Committee. Does government have a response to concerns that fees are levied too often?

- Section 5 of the Act dictates that a request must provide sufficient detail to enable an experienced employee of the public body, with a reasonable effort, to identify the records sought.
- As the number of over-broad requests continues to increase, which directly correlates to the issuance of fees, government recognizes that applicants may need more clarity regarding the kind of information that needs to be provided to allow government to conduct a meaningful and timely search for the requested records.

s.13

- As per FOIPPA's fee schedule, the first 3 hours of search for records are free. Government charges applicants for search time above the 3 hours; for time spent preparing records for disclosure, i.e. scanning and photo copying; and for any disks or storage devices required to

get the records to the applicant. Government does not charge applicants for the time spent severing a record.

- Last fiscal, IAO recovered approximately $80,000 from FOI fees.

FOI COSTS

Q: What are the costs to government for processing FOI requests?

- In their most recent calculations (FY1314), Information Access Operations estimated that the average cost of processing an FOI request was $2,015. This figure is derived from budget numbers and the number of closed requests.
- This places the estimated total cost to government at nearly $20 million.
- IAO estimates that since centralization in 2009 the cost to respond to an FOI request has dropped by more than half. This is a credit to the ongoing efforts by public body and IAO staff to streamline FOI processes.

FREQUENCY OF SPECIAL COMMITTEE

Q: As part of their submission, the OIPC has recommended that section 80 (1) of FIPPA be amended to change the review cycle from 6 years to every 3-4 years. Will government consider such an amendment?

s.13

DATA LINKING

Q: We understand that data linking has been an issue of contention between public bodies and the OIPC. Has government found a solution?

- During the development of the data linking regulations in 2012, the OIPC expressed concern that the data linking definitions in FOIPPA were too narrow to encompass the range of activities that should be subject to OIPC oversight and to the applicable regulations.
- Government has since worked with the OIPC to develop broader definitions which cover an appropriate range of activities.
- Government's plans in this area were discussed by Bette-Jo Hughes in government's previous submission to the Special Committee.

MANDATORY BREACH NOTIFICATION

Q: The OIPC has recommended amendments to FOIPPA to include a mandatory requirement for notification in the event of privacy breach. As the issue of privacy breaches in government has taken centre stage of late, will government act on this recommendation?

- The Special Committees that reviewed PIPA, B.C.'s private sector privacy legislation, in 2008 and 2015, recommended that a mandatory requirement for privacy breach notifications be incorporated into the Act.
- The OIPC has been supportive of this recommendation and, as you have stated, has asked government to enshrine mandatory breach notifications within FOIPPA as well.
- Currently, government provides monthly reports to the OIPC about each privacy incident investigated by the Privacy, Compliance and Training Branch and continues to report "serious" privacy breaches to the OIPC within a few days of occurrence.
- Moving forward, government has committed to addressing the 2008 and 2015 Special Committee recommendation for mandatory breach notification within PIPA at the next available legislative opportunity and welcomes any similar recommendations for FOIPPA.

ABORTION SERVICES PROVISION

Q: The Special Committee received several submissions calling for changes to section 22.1 of FOIPPA. Will government consider these recommendations?

- Before considering any change to a mandatory exception of this nature, we would first need to go back and analyze the rationale for implementing this provision in the first place.
- Protecting the privacy of BC citizens is government's top priority.

SECTION 13 – POLICY ADVICE OR RECOMMENDATIONS

Q: There is considerable interest in amending section 13. Advocacy groups, the OIPC and some committee members were all in favour of a narrower definition of "policy advice". Does government plan to act on these recommendations?

- This issue has come up during past Special Committee reviews. In 2010, the Commissioner made a recommendation that section 13 be narrowed, but the Special Committee declined to make a recommendation in this regard.
- A 2014 Ontario Supreme Court decision supports BC's section 13 as it is currently written. In this decision, the Supreme Court states that Ontario's section 13, which is very similar to BC's provision, accords with the balance struck by the legislature between the goal of preserving an effective public service capable of producing full, free and frank advice and the goal of providing a meaningful right of access.
- BC's discretionary exception relating to advice and recommendations aligns closely with most jurisdictions in Canada and is markedly similar to that of the Yukon, Newfoundland and Labrador, Ontario and the federal access to information legislation.

RESTRICTIONS ON PUBLISHING REPORTS

Q: The Commissioner has raised the issue of the restrictions placed on publishing investigatory reports. Does government plan to address this issue for the sake of transparency?

- This issue relates to section 30.1 of FOIPPA, which states that public bodies are required to store and access personal information only within Canada.
- Publishing these types of investigatory reports online is effectively a disclosure outside of Canada and as the bulk of these reports include personal information, this would represent a contravention of the Act.
- Government remains mindful of the need for openness and transparency, and recognizes that the contents of these reports are often of interest to the public.
- The Commissioner has posed a solution to this issue, which government has considered and supports.

EMPLOYEE ETHICS

Q: How do we know that government employees take their information management obligations seriously?

- The Appropriate Use of Government Information and Information Technology Policy clearly lays out the requirements for employees who collect, use, disclose and dispose of government information.
- Employees are made aware of their obligation to handle information in a manner that meets the requirements of FOIPPA, the DDA, and — when in force — the IMA.
- Employees who fail to comply with these standards are subject to disciplinary action up to and including dismissal. This includes employees who wilfully destroy government information that should not be destroyed (whether or not it is the subject of an FOI request).
- This policy is supported by the Standards of Conduct, which requires employees to conduct themselves in a manner that will instill confidence and trust and not bring the B.C. Public Service into disrepute.
- Government expects employees to act in an ethical manner, and the recent Workplace Environment Survey indicates that employees are

aware of and complying with this expectation. Specifically, the survey polled employees on whether they feel that they are clear on what ethical values are expected when performing their work, and whether they feel supported in carrying out their work in an ethical manner. Nearly 80% of employees agreed with both of these statements, while less than 10% disagreed.

COMMISSIONER OVERSIGHT OF IMA

Q. Why do you not support independent oversight of the information management Act and other information management requirements by the Commissioner similar to Alberta?

- Other than Alberta, no other jurisdiction in Canada provides their Commissioner with this type of oversight.
- In most cases, this type of oversight exists within the relevant records management legislation in most other Canadian jurisdictions.

TRANSITORY RECORDS

Q. The Commissioner and David Loukidelis have, in their respective recent reports, identified the need for greater clarity for government employees respecting what constitutes a transitory record. What is government doing about this?

- Transitory records have temporary usefulness, and are only needed for a limited period of time in order to complete a routine action or prepare a final record, such as meeting arrangements, copies created for the convenience of an employee, or drafts.
- Transitory records are not required for any government financial, legal, audit or statutory purpose, and are not required to be filed and kept in government recordkeeping systems.
- Currently, government employees are provided with training and an online guide which explains what are and are not transitory records.
- The Province is developing expanded transitory records guidance and training for all employees. The new training program, which is currently under development, will enhance government employees' knowledge so they are better able to distinguish between records that

must be retained and records that are transitory, regardless of format (i.e., including email).

- Government is in the process of reviewing its management of all records including transitory records as well as those that government needs to keep for business, legal or historical/archival reasons.

SAVING OF E-MAILS

Q. What is Government doing to ensure that employees do not inappropriately delete e-mails, and what impact could this have on Freedom of Information requests?

- On December 16, 2015, Premier Clark announced that the practice of "triple-deleting" e-mails is prohibited in Government, and that ministers and political staff are to continue to retain all their sent e-mails until further notice.
- The same day, John Dyble, Head of the Public Service, provided interim guidance to public employees, including information relating to both e-mail and transitory records.
- The Premier's original direction to ministers and political staff to retain sent e-mail was issued on October 23, 2015.
- Further, Government is developing new guidance and training material, which will clarify what records are transitory and other information that is important to the appropriate management of e-mail. This training will be delivered to all employees beginning in April and concluding by the end of the fiscal year.

Issue	Brief Description
OIPC	
Subsidiary Corporations	The OIPC and several other stakeholders have recommended that FOIPPA be amended to bring subsidiaries of public bodies under FOIPPA. Specifically, the OIPC has recommended moving paragraph (n) of the definition of “local government body” into the definition of “public body” in Schedule I, so that entities such as subsidiaries of educational bodies and the BCACP fall within the scope of FIPPA.
Mandatory Breach Reporting	The Commissioner's office has recommended to the Special Committee that FOIPPA be amended to include a mandatory requirement for government to report all privacy breaches to the OIPC as well as to the impacted individuals if the breach or suspected breach could reasonably be expected to cause harm to an individual and/or involves a large number of individuals;
Duty to Document	A recommendation has been made by the OIPC to add to Part 2 of FIPPA a duty for public bodies to document key actions and decisions based on the definition of “government information” in the Information Management Act.
Expand Commissioner Oversight	The OIPC has called for amendments to section 42 of FOIPPA to expand the Commissioner’s oversight by granting the Commissioner the jurisdiction to review matters or allegations of unauthorized destruction of records.
Other Stakeholders	
Access Fees	Several stakeholders, including the Center for Law and Democracy have called for a reduction or elimination of fees for access requests.
Data Residency	Submissions from several stakeholder groups, including BC health authorities and the College for Registered Nurses have highlighted the limitations that the current data residency provisions in FOIPPA, specifically section 30.1, place on their operations. These stakeholders are calling for an expansion to the list of exceptions to this provision, which states that personal information must be stored and accessed in Canada only.
"Public Interest" Disclosure Provision	A number of stakeholders spoke in favor of the OIPC's recent interpretation of section 25, which removes the element of temporal urgency when considering disclosure in the public interest. In addition, some stakeholders recommended that this provision be amended to expand its application.

Subsidiary Corporations recommendation

Recommendation (#3):

The OIPC recommended: Amend FIPPA to move paragraph (n) of the definition of "local government body" into the definition of "public body" in Schedule 1, so that entities such as subsidiaries of educational bodies and the BCACP fall within the scope of FIPPA.

Rationale:

The Commissioner has stated that "Corporations or other organizations set up by public bodies are conducting public business. As such they should be subjected to FIPPA and held accountable for their use of public resources. This will improve accountability and transparency for the public and create consistency with the requirements for local government bodies."

Effect:

s.13

Summary of OIPC Recommendations and Status of Government's Response

Document	OIPC Recommendation	OIPC current appraisal and concerns	Government's Response
DATA-LINKING	An error in the drafting of the definition for data linking has resulted in very few initiatives being subject to OIPC oversight. The definition should be broadened to include the type of initiatives that were originally intended to be covered by the 2011 FOIPPA amendments. As acknowledged by Deputy Minister Kim Henderson in her April 11, 2013 letter to the Commissioner, the data linking provisions as currently drafted do not achieve their intended policy objectives and this matter should addressed at the earliest opportunity.	s.12	
INVESTIGATION REPORTS			
F11-02 – BC FERRIES (MAY 2011)	Minimum delay of 24 hours between the applicant's receipt of the response and the time the response is publicly posted.	This report was re BC Ferries, but government instituted a 72-hour delay.	Government acted on this recommendation in a manner favourable to applicants by implementing a longer delay between when the applicant received their response and when the response was publicly posted.
F13-01 – INCREASE IN NO RESPONSIVE RECORDS (MARCH 2013)	IAO communicate to an applicant when it is aware that the records the applicant is seeking exist within a different ministry than from where the applicant has originally requested the records.	Accepted by government.	Government has implemented this recommendation.
	IAO should be reasonably confident that before narrowing a request, the result will not deprive	Accepted by government.	Government has implemented this recommendation.

Summary of OIPC Recommendations and Status of Government's Response

	applicants of records they would otherwise receive, unless IAO informs the applicant that this may be the case.		
	IAO ensure that it interprets requests broadly enough to assist the applicants in obtaining the records he or she is seeking.	Accepted by government.	Government has implemented this recommendation.
	Where government does not have records responsive to an access request, IAO provide an explanation to the applicant as to why this is the case.	Accepted by government. We still see instances where this is not done. Same recommendation made in 2014 timeliness report.	IAO works closely with program areas to provide details to applicants on no records responses wherever possible.
	IAO develop a classification system that more accurately reflects where an individual who has made the same request to multiple ministries ultimately receives the records they were seeking, irrespective of how many ministries respond that they do not have records.	Accepted by government.	Government has implemented this recommendation by creating a new disposition to note where records requested were located in another ministry.
	Government create a legislative duty to document key decisions as a clear indication that it does not endorse "oral government" and that it is committed to be accountable to citizens by creating an accurate record of its actions.	No position taken to date. Recommendation also made in various letters to Minister and within consult on draft Information Management Act.	Government has taken this recommendation under consideration. s.13 s.13
F13-03: Evaluating the Government of BC's Open Government Initiative (July 25th, 2013)	• All ministries should implement s. 71 of FOIPPA without further delay and establish categories of records for disclosure on a proactive basis. These obligations should be made part of letters	Accepted. No action taken.	Consultation with ministries to design a standardized approach across government has been conducted. MTICS is currently

	of expectation for ministers and deputy ministers.		exploring options for implementation and potential additional consultation if required. Government will be proactively releasing purchasing card data for all ministries as open data at the end of January, which establishes a new category.
	• The minister responsible for FOIPPA should direct ministries to proactively disclose the travel and hospitality expenses of ministers, deputy ministers and assistant deputy ministers or their equivalent by purpose or event. The disclosed information should include the date of the event, destination, and expenses relating to flight, other transportation, accommodations, meals and incidentals, and the total amount spent for that particular purpose or event. This information should be published and searchable in an open data format.	No position taken. No action taken.	MTICS is assessing additional categories of information that can be proactively released and will be putting options forward for decision.
	• The minister responsible for FOIPPA should direct ministries to proactively disclose calendar information of ministers, deputy ministers and senior executives or equivalent. This release should contain the names of participants, the subject and date of external meetings and be published, at minimum, on a monthly basis.	No position taken. No action taken.	Government is continuing to consider the benefits of proactive release for calendars given that there is currently only one applicant requesting this information. Government must also consider the security implications that may occur from broader release.
	• The minister responsible for FOIPPA should direct ministries to proactively disclose	No position taken. No action taken.	MTICS is assessing additional categories of information that can

Summary of OIPC Recommendations and Status of Government's Response

	information relating to its contracts that are worth more than $10,000 on (at minimum) a quarterly basis. Contract information should include with whom the government is contracting, the purpose, value and duration of that contract, and information about the procurement process for the award of the contract.		be proactively released and will be putting options forward for decision.
	• The minister responsible for FOIPPA should direct ministries to proactively disclose any final report or audit on the performance or efficiency of their policies, programs or activities.	No position taken. No action taken.	MTICS is assessing additional categories of information that can be proactively released and will be putting options forward for decision.
	• The minister responsible for FOIPPA should direct ministries to proactively disclose the records enumerated in s. 13(2) of FIPPA on a routine basis within a set timeline.	No position taken. No action taken.	MTICS is assessing additional categories of information that can be proactively released and will be putting options forward for decision.
	• The Open Information website should be used as an online library to make information that must be disclosed across government more easily accessible by providing links to that information or a search function.	Under consideration by government. Last update was that government was pursuing this recommendation. Require update on implementation.	Government launched a comprehensive web consolidation project in October 2013 through which ministries will migrate all of the content and documents to a shared web publishing platform. The will significantly improve the findability and accessibility of all government information published online.
	• Government should create a separate category for records that are not published on the	Accepted. Government said they	IAO is currently transitioning to new FOI software and will create

Summary of OIPC Recommendations and Status of Government's Response

	disclosure log due to concerns about copyright.	would create this category and it would be included in the next revision of policy. We would like to see it.	a new category within that system to identify records that are not published due to copyright concerns.
	• Government should review its policy regarding the disclosure of copyright material to determine whether it is permissible to publish copyright material in response to an access request. Where it is determined that records may not be published due to copyright, government should publish a severed version of the record.	Accepted by government. We would like an updated on implementation.	MTICS is examining updates to the Open Information and Open Data Policy to ensure it stays up-to-date with evolving needs of government and citizens. Any additional work undertaken at IAO to re-sever access requests must be balanced with meeting legislated timelines on current open requests.
	• Government should include information on the Open Information website and in the annual report of the Minister of Technology, Innovation and Citizens' Services regarding responses to general access requests where there have been no responsive records.	Accepted by government. We would like an update on implementation.	Information about the number of no-records responses is included in the annual report on the FOIPP Act. Data on all requests, including no records responses is posted quarterly to DataBC.
	• Government should improve the ability to search the disclosure log to allow users to find specific content more easily.	Accepted by government. We would like an update on implementation.	Improvements have been made to the ability to search for content on Open Information, as well as other websites under the gov.bc.ca model.
	• Government should identify high value data sets for publication, particularly those that will increase the transparency and accountability of	Tentative acceptance by government. DataBC Council	Government is engaging business and industry to help determine high-value data. Work is also

Summary of OIPC Recommendations and Status of Government's Response

	government and work towards releasing all identified high value data sets as soon as practicable.	agreed to make changes that government believed would address this. We would like an update on implementation.	underway to design a comprehensive approach to cataloguing government data assets.
	• Government should commit to signing and implementing the G8 Open Data Charter as a sub-national.	Tentative acceptance by government. We would like an update on implementation.	The categories of data listed in the G8 Open data Charter are being considered for use in developing the catalogue of government data assets.
	• Government should develop a single de-identification approach for ministries that includes procedures on de-identifying datasets and assessing the risk of re-identification in the context of open data. • Government should also develop policies for reviewing data released as open data on a regular basis to assess the risk of re-identification.	Tentative acceptance by government. DataBC Council agreed to make changes that government believed would address this. We would like an update on implementation.	The Privacy and Legislation Branch is researching de-identification processes. As part of the Open Information and Open Data Policy, data sets that have the potential to include personal information must be vetted by the Privacy and Legislation Branch prior to being posted.
	• Government should continue to collaborate with stakeholders to increase data literacy and data literacy should be considered a measure of success for the open data program.	Tentative acceptance by government. DataBC Council agreed to make changes that government believed would address this. We would like an	Collaboration efforts inside and outside government emphasize data literacy and the power of data to support decision making. This work includes direct ministry outreach on data literacy, as well as public facing work via the DataBC blog highlighting

Summary of OIPC Recommendations and Status of Government's Response

		update on implementation.	important data oriented work.
	• Government should incorporate access by design principles into its information management practices.	Tentative acceptance by government. We would like an update on implementation.	The Privacy and Legislation Branch is developing an access-by-design assessment to include in the initial review that all project, programs, systems and legislation are required to undergo.
	• Government should establish an external advisory board on open government comprised of users of open information and open data, as well as, data and privacy experts to inform future developments in open government.	Under consideration. We would like an update on implementation.	The DataBC program is exploring options to engage business and industry to understand their views on access, use and value of data. It is anticipated this will include key players in the open data community.
	• The Document Disposal Act should be replaced with a modern archives and records management statute. • The government also should act now to develop an archiving policy for its Open Information website, to enable citizens to continue to access records that have been removed from the active site. Indices of archives and the policy should be posted on the Open Information website.	Accepted by government. Accepted by government. We would like an update on implementation.	This is being addressed by the proposed new Information Management Act. Government has changed its archiving policy and no longer requires a two year limitation on information posted to Open Information.
F13-04 – Sharing of Personal Information as part of the Draft Multicultural Strategic	• Government should provide training for its employees regarding the use of personal email accounts.	Accepted. We would like an update on implementation.	Addressed through the implementation of the "Appropriate Use" policy.

Summary of OIPC Recommendations and Status of Government's Response

Outreach Plan (August 2013)			
	• Government should ensure that copies of all records created by its employees that relate to government business are located in government-controlled information management systems	Accepted. We would like an update on implementation.	Addressed through the implementation of the new "Appropriate Use" policy
	• Government should provide its employees with sufficient technical resources to ensure that they do not have a reason to use personal email accounts in the performance of their government duties.	Accepted. We would like an update on implementation.	Addressed through the implementation of the "Appropriate Use" policy.
	• Government should ensure that employees with roles that are closely tied to the governing party participate in mandatory training sessions regarding the need to keep personal information obtained in their government role separate from personal information obtained in any role they might have with the political party.	Accepted. We would like an update on implementation.	Addressed through the implementation of the "Appropriate Use" policy. Training on this policy has taken place in 2014 and will continue to be offered to all government employees. In addition, on-going, in person training on records management and access is delivered to new government employees on an as and when needed basis.
Investigation Report F13-05: Pubic Body Disclosure of Information Under Section 25 of the *Freedom of Information and Protection of Privacy Act*	Public bodies should develop policies that provide guidance to employees and officers about the public body's obligations under s. 25 of FIPPA. •	No position taken. Has any action been taken?	OCIO has developed and distributed a guidance document with respect to s.25.

Summary of OIPC Recommendations and Status of Government's Response

(Dec. 2, 2013)			
	Public bodies should ensure that its employees and officers understand the public body's obligations under s. 25 of FIPPA and are provided with adequate training to ensure compliance with these obligations	No position taken. Has any action been taken?	OCIO has developed and distributed a guidance document with respect to s.25 and has increased the discussion of s.25 in all the general FOIPPA training sessions.
	Government should amend s. 25(1)(b) of FOIPPA to remove the requirement of temporal urgency so that there is a mandatory obligation for public bodies to disclose all information that is clearly in the public interest to disclose.	No position taken. Does government have a position on this recommendation?	The implications of this change require further investigation.
F14-01: Use of Police Information Checks in British Columbia (Apr. 15, 2014)	• Government and municipal police boards should immediately mandate that police apprehensions collected under the authority of s. 28 of the Mental Health Act should never be included in a police information check.		To support the province's police agencies in providing a common and consistent approach to record checks, the Ministry of Justice developed model policy guidelines that detail what information should and should not be released for those working with the vulnerable sector and those seeking employment that do not work directly with the vulnerable sector. The BC Association of Chiefs of Police has endorsed the policy. The model policy guidelines state that s. 28 information should not be disclosed.
	• Government should legislatively mandate that		To support the province's police

	non-conviction information cannot be used in record checks outside of the vulnerable sector.		agencies in providing a common and consistent approach to record checks, the Ministry of Justice developed model policy guidelines that detail what information should and should not be released for those working with the vulnerable sector and those seeking employment that do not work directly with the vulnerable sector. The BC Association of Chiefs of Police has endorsed this policy. The model policy guidelines state that non-conviction information should not be disclosed outside of the vulnerable sector.
	• At the direction of government and municipal police boards, police agencies should implement a model for conducting record checks that will allow individuals to request only relevant conviction information for record checks for positions outside of the vulnerable sector.		Federal Canadian Police Information Centre (CPIC) policy does not allow for the partial disclosure of an individual's criminal record. This recommendation cannot be actioned at this time.
	• Government should legislatively mandate that the centralized office in place under the CRRA should conduct all vulnerable sector checks in British Columbia. The current process for mandatory checks under the CRRA for provincially-funded employers would remain the same. Where an employer or volunteer agency		s.13

	that is not currently subject to the CRRA chooses to require a prospective employee or volunteer in the vulnerable sector to undergo a record check, it would be conducted in the same manner as set out by the CRRA.		
	• Government and municipal police boards should direct municipal police departments to immediately stop releasing non-conviction information for police information checks not involving the vulnerable sector.		To support the province's police agencies in providing a common and consistent approach to record checks, the Ministry of Justice developed model policy guidelines that detail what information should and should not be released for those working with the vulnerable sector and those seeking employment that do not work directly with the vulnerable sector. The BC Association of Chiefs of Police has endorsed this policy. The model policy guidelines state that non-conviction information should not be disclosed outside of the vulnerable sector.
F15-02 Review of the Mount Polley Mine Tailings Pond Failure and Public Interest Disclosure by Public Bodies	• I recommend that the Ministry of Energy and Mines and the Ministry of Environment promptly assess what information in relation to the failure of the Mount Polley tailings pond dam, if any, must be disclosed pursuant to s. 25(1)(b) as being clearly in the public interest.	Pending	The Ministry is currently working to understand the new interpretation of section 25(1)(b), and determining how this new interpretation should be applied to records relating to Mount Polley.

Summary of OIPC Recommendations and Status of Government's Response

	• I recommend that all public bodies diligently and promptly assess what information, if any, must be disclosed pursuant to s. 25(1)(b) as being clearly in the public interest.	Pending	Government has taken this recommendation under consideration.
	• All public bodies must develop policies that provide guidance to employees and officers about the public body's obligations under s. 25 of FIPPA, and update existing policies to reflect the revised interpretation of s. 25(1)(b) described in the investigation report. *"I conclude that public bodies must disclose information pursuant to s. 25(1)(b) where a disinterested and reasonable observer, knowing what the information is and knowing all of the circumstances, would conclude that disclosure is plainly and obviously in the public interest. Section 25(1)(b) will no longer be interpreted to require an element of temporal urgency in order to require the disclosure of information that is clearly in the public interest pursuant to s. 25(1)(b)."*	Pending	The implications of this change in interpretation require further investigation.
F15-03 Access Denied: Record Retention and Disposal Practices of the Government of British Columbia	• The Ministry of Transportation and Infrastructure should release the 36 pages of records initially identified as responsive to the applicant's access request, with severing as allowed under FIPPA, made on November 19, 2014 for: ○ "… all government records that make reference to the issue of missing women along Highway 16 / the Highway of Tears and specifically including records	Pending	Government has engaged David Loukidelis, former Information and Privacy Commissioner and former Deputy Attorney General to assist government in ensuring a common application of the rules under FOIPPA and that staff across government are properly trained in application of these rules. We look forward to

	related to meetings held by the ministry on this issue. The time frame for my request is May 15 to November 19, 2014."		recommendations Mr. Loukidelis will make in this regard.
	• Government should develop a policy for all future data migrations that requires at a minimum: 1. Hourly, daily and monthly backup of data; 2. Written directions to government's service provider with respect to these backups; and 3. Government monitoring of the directions to ensure their compliance.	As above	Pending
	• The Ministry of Advanced Education should release the approximately 20 email records identified as responsive to the applicant's access request, with severing as allowed under FIPPA, made on July 21, 2014 for: ○ "Any emails sent by Nick Facey, Chief of Staff to Minister Amrik Virk. Timeframe is February 1, 2014 to July 16, 2014." ○ The Investigations and Forensics Unit will retrieve the emails and provide them to the Ministry.	As above	Pending
	• The Executive Branch of the Office of the Premier should change its access to information processes to ensure that requests for records are communicated by email in a timely manner and properly documented.	As above	Pending
	• Government should clarify access requests with	As above	Pending

	applicants where necessary to ensure it does not interpret the request too narrowly and to maximize the likelihood of producing records that are responsive to the applicant's request.		
	• Government should create clear guidance for employees on how to conduct a thorough search for potentially responsive records to an access request. This guidance should be incorporated into government's access to information training and should specifically include that employees should conduct searches from their desktop or laptop and not from mobile devices.	As above	Pending
	• Government should provide mandatory records management training to all employees, that includes the identification of transitory and non-transitory records and the process for retaining and destroying records. This training should describe employees' responsibilities for records management and provide the basis for understanding an office's record keeping system.	As above	Pending
	• Government should legislate independent oversight of information management requirements, such as the destruction of records, including sanctions when those requirements are not met.	As above	Pending
	• Government should configure the settings in Microsoft Outlook to prevent employees from removing items from the Recover Deleted Items folder.	As above	Pending

Summary of OIPC Recommendations and Status of Government's Response

	• Government should configure the settings in Microsoft Outlook so that it preserves items in the Recover Deleted Items folder for just over one month. This would ensure all government emails are captured in monthly backups.	As above	Pending
	• Government should create a legislative duty to document within FIPPA as a clear indication that it does not endorse "oral government" and that it is committed to be accountable to citizens by creating an accurate record of its key decisions and actions.	As above	Pending
Special Reports			
A Failure to Archive – Recommendations to Modernize Government Records Management (July 22, 2014)	• Government should repatriate the BC Archives into government and fund it on the same basis as other valuable public programs. • Alternatively, government should develop a policy or legislative framework where the fees to archive records are set on a basis that is acceptable to both government and the Royal British Columbia Museum rather than the current unilateral process set by the Museum. Ministries should then be provided with sufficient resources to enable the transfer of records to the BC Archives. • To address the backlog of 33,000 boxes of records, government should provide funding to the Royal British Columbia Museum from the 2014/15 Estimates – Contingencies in an amount to be determined.	No position taken The proposed Information Management Act creates a bifurcated archive system. While it proposes a Digital archive going forward, the museum has paper records and a backlog.	The creation of a government digital archive, in the proposed Information Management Act, partially addresses the recommendation to bring the Archives back into Government. The Royal BC Museum and the Government (MTICS/CSCD) have set up a joint committee which is actively identifying feasible options for the transfer of backlog and future records to archival custody.
	• The Minister of Technology, Innovation and Citizens' Services should initiate the creation or	Accepted by government.	Met through the proposed Information Management Act.

Summary of OIPC Recommendations and Status of Government's Response

	procurement of an electronic records archiving infrastructure to ensure the management and archival preservation of government's electronic records. • The repository for the electronic archives should be within the Ministry and should be publically funded.	Provision exists in the Information Management Act	
	• Recognizing changes in information management in the last decade, Government should replace the Document Disposal Act of 1936 with a modern statutory framework to address the needs and realities of the digital age.		Met through the proposed Information Management Act
	• Provincial archivist should play a prominent role in decisions around the creation of electronic records as well as the approval of retention schedules.	No position taken. Not addressed in the Information Management Act.	Addressed through the proposed Information Management Act. The IMA establishes a Chief Records Officer who has responsibility for approving information retention schedules and has authority to issue directions to government bodies regarding the digitization of information. The CRO's role is equivalent to the role assigned to a provincial archivist in other legislation.
	• Process for approval of records schedules should be more efficient and should not require the approval of the Legislature of the Public Accounts Committee.	No position taken. The draft Information Management Act attempts to address	Addressed through the proposed Information Management Act. This Act will eliminate the need for approval of the legislature by the Public Documents Committee.

Summary of OIPC Recommendations and Status of Government's Response

			Approval processes will be streamlined and accomplished through the creation of a Chief Records Officer.
	• Should provide for oversight of information management requirements and for sanctions when those requirements are not met.	s.13	
A Step Backwards: Report Card on Government's Access to Information Responses April 1, 2013 – March 31, 2014 (Sept. 23, 2014)	• Government should define and implement steps to eliminate the backlog of access to information requests and, in the forthcoming budget cycle, should give priority to providing more resources to dealing with the greatly increased volume of access requests.	No position taken. We would like an update on government's position and any steps being taken.	IAO is taking steps to reduce the overdue backlog while continuing to provide timely responses to current requests. Resources have been reallocated within the current budget envelope to address areas of high volume. Timeliness is up overall this year from 74% to 80%.
	• As recommended in my report entitled A Failure to Archive: Recommendations to Modernize Government Information Management, government should adopt a modern statutory framework to address the needs and realities of the digital age, recognizing the importance for government to effectively track records from	Accepted by government. IMA largely accomplishes this.	Met through the proposed Information Management Act

	their creation through to their archiving.		
	• After discussion and agreement between government and the political parties currently making calendar requests, the minister responsible for FOIPPA should develop a system to proactively disclose calendar information of ministers, deputy ministers, assistant deputy ministers, as well as, certain other staff whose calendars are routinely the subject of access to information requests. This release should, at a minimum, contain the names of participants, the subject and date of meetings and be published on a monthly basis.	No position taken. Would appreciate an update.	Government is continuing to consider the benefits of proactive release for calendars given that there is currently only one applicant requesting this information. Government must also consider the security implications that may occur from broader release.
	• The Ministry of Children and Family Development should give attention on a priority basis to its statutory obligation under FOIPPA to respond to access to information requests within legal timelines. Planned actions should include addressing elements such as printing and retrieving difficulties regarding the ICM system, staff levels related to access to information and providing effective ongoing training to ICM users.		MCFD is moving forward with the final phase of ICM, which includes systems enhancement to facilitate access. MCFD will also be providing training to approximately 2,700 employees on the latest changes.
	Government should ensure it builds access and privacy into any new information management system at the design stage in order to ensure the system operates from a records management perspective, as well as, from a program perspective.	No position taken. Forward-looking.	Government's current privacy impact assessment process looks to ensure that privacy is built into any new system or program during the development phase. PIA completion continues to climb

Summary of OIPC Recommendations and Status of Government's Response

			across government. A Data and Access Assessment is currently under development to help ensure that program areas turn their attention to how data will be made open and accessible in any new system or program.
	Where government does not have records responsive to an access to information request, IAO should provide a brief explanation to the applicant as to why this is the case.	No position taken. Forward-looking but would like an update.	This recommendation was also made in the "Increase in No Responsive Records" investigation report and has been adopted by IAO.
	Government should implement the Capstone or a similar email management system with respect to senior government officials to document its key decisions. This system should also be adopted by the Office of the Premier and Ministerial offices.	No position taken. Not included in draft IMA.	Government is currently considering tools (e.g., auto-classification pilot) to facilitate effective e-mail management. The existing Executive Records Schedule resembles the Capstone approach with respect to ADMs and above.
An Examination of The Government of BC'S Privacy Breach Management (January 2015)	Government establish an ongoing privacy compliance monitoring function within the OCIO that: a.) Reviews processes, policies & training government-wide, to ensure that breaches are promptly reported to the OCIO and that affected individuals are notified without delay; b.) Conducts regular follow-up with ministries to ensure full implementation of prevention strategies and recommendations provided through the breach	Accepted (in conversation rather than letter). We will need to follow-up re implementation and may need clarification on their position.	Accepted in principle. A corporate Privacy Management and Accountability Policy has been developed and is being gradually implemented. A compliance monitoring plan which is a key component of this policy is expected to be implemented late 2015.

Summary of OIPC Recommendations and Status of Government's Response

	investigation process; c.) Reviews privacy and security safeguards within ministries and service providers; d.) Conducts regular cross-government analysis of the causes and potential solutions to privacy breaches; and e.) Publicly reports detailed information relating to breaches, bodies, responsibilities, types and causes, and preventative measures annually.		In addition, government is undertaking a business requirements analysis for a new information management system that will improve data collection, analytics and reporting. Further opportunities for public reporting are under consideration.
	Government adopt the following interim breach reporting requirements: a.) Document risk evaluation processes and decisions regarding notification of affected individuals and reporting to the OIPC; and b.) Report all suspected breaches to the OIPC if the suspected breach: - Involves personal information; and - Could reasonably be expected to cause injury or harm to the individual and/or involves a large number of individuals.	Under consideration. Government is considering resource implications.	Government needs to conduct a further review of this recommendation along with further discussions with the Commissioner's office. The goal is to add value to the process within the current resource allocations that are available.
	The OCIO to: a.) Review and amend breach categories and category definitions; b.) Ensure fulsome and accurate collection and documentation of privacy breach incidents; c.) Ensure ministry tracking of the OCIO file number; and d.) Ensure OCIO tracking of the OIPC file number.	Under consideration. Government is considering resource implications.	Government needs to conduct a further review of this recommendation along with further discussions with the Commissioner's office. The goal is to add value to the process within the current resource allocations that are available.
	The OCIO to: a.) Review and amend policy documents relating to	Accepted (in conversation rather	Government accepts in principle. Refinements and changes to the

	privacy breach management; and b.) Provide basic guidance or training for privacy breach investigative staff as well as ministry information and security staff relating to amendments made.	than letter). We will need to follow-up re implementation and may need clarification on their position.	centralized privacy breach management practices are now being incorporated into a new policy document which will establish an updated governance framework for the operations of the privacy breach management unit. Once the policy is updated, basic training about the changes will be provided to the privacy breach investigative unit and ministry staff.
	Government to: a.) Provide ongoing training and awareness of the importance of protecting personal information and breach management processes; and b.) Increase staff (and service provider, if applicable) participation rates in this training.	Accepted (in conversation rather than letter). We will need to follow-up re implementation and may need clarification on their position.	Government accepts in principle. As of January 2015, more than 72.8 per cent of all government employees (including 86.7 per cent of all government executives) completed government's mandatory privacy breach training course. Government continues efforts to increase completion rates. In addition, the OCIO is developing an online privacy training course for government contractors and service providers which should be fully implemented this Spring.

Summary of OIPC Recommendations and Status of Government's Response

OTHER			
Subsidiary Corporations (various letters, including June 11, 2014)	We have asked that government amend FIPPA to ensure that subsidiary corporations of local public bodies are covered.	Under consideration Response from Minister Wilkinson at end of July 2014 saying government continues to consult with stakeholders. We would appreciate an update.	Consultations have indicated that this is a complex issue due to the divergent types of corporations that are affiliated with local public bodies. Further review and consideration is required.
Adding PRIMECorp to Schedule 2 (2012)	We asked for PRIMECorp to be added	Accepted. Added in 2013.	Completed. Was added to Schedule 2 in 2013.
BC Services Card (Feb. 2013)	We recommended public consultation about the implementation of BC Services Card.	Adopted. Completed.	Government completed public consultation on the initial implementation of the BC Services Card.
Statement from BC Privacy Commissioner regarding the results of government's public consultation on the BC Services Card (Apr 1, 2014)	The need for public consultation on the BC Services Card is not over. Future public consultations are required as the system is architected and new services are contemplated.		A stakeholder engagement strategy and approach document is currently under development and will be completed by April 15, 2015.
Open Letter to Minister Wilkinson regarding the designation of police associations as public bodies under FOIPPA. (Apr. 2, 2014)	Recommend that the BC Association of Chiefs of Police and the BC Association of Municipal Chiefs of Police be added as public bodies under FOIPPA.	Under consideration. Is there any update on this?	s.12,s.13

Summary of OIPC Recommendations and Status of Government's Response

			s.13

Berglund, Lara FIN:EX

From: Reed, Matt MTIC:EX
Sent: Thursday, March 3, 2016 2:05 PM
To: Sime, Mark MTIC:EX
Cc: Plater, Sharon MTIC:EX
Subject: Fwd: Feedback from Cheryl on Special Committee Submission Outline

Mark - can you action this right away please?
Sharon - no need to review what we have sent you already but Mark will have some questions on the new content we need to provide
-m

Sent from my phone

Begin forwarded message:

> **From:** "Lowe, Charmaine MTIC:EX" <charmaine.lowe@gov.bc.ca>
> **Date:** March 3, 2016 at 1:37:03 PM PST
> **To:** "Reed, Matt MTIC:EX" <Matt.Reed@gov.bc.ca>, "Sexsmith, Melissa M MTIC:EX" <Melissa.M.Sexsmith@gov.bc.ca>, "Rice, Colleen A MTIC:EX" <Colleen.Rice@gov.bc.ca>, "Plater, Carmelina MTIC:EX" <Carmelina.Plater@gov.bc.ca>
> **Subject: Feedback from Cheryl on Special Committee Submission Outline**
>
> s.13

Matt, For your pieces in particular, I did mention that I wasn't sure how much of this you had already and that we may not be able to gather all of this additional material in the short term. If that is the case, you might want to let Sharon know who can convey that to Cheryl.
Thanks everyone.
Charmaine

From:	Macdonald, Scott
To:	Reed, Matt MTIC:EX
Subject:	RE: special committee content
Date:	Thursday, January 21, 2016 3:43:11 PM
Attachments:	image001.jpg

Thank you, Matt. This is very helpful and I would appreciate hearing about any briefing developments that you are at liberty to share.
SM

From: Reed, Matt MTIC:EX [mailto:Matt.Reed@gov.bc.ca]
Sent: 2016, January 21 2:15 PM
To: Macdonald, Scott
Subject: special committee content

Hi Scott,

As promised, here are the references that were made to the Special Committee on subsidiary corporations:

From the transcripts of the in-person consultations:

From Rob Wipond (page 129):

Subsidiaries. This issue has been brought up to you repeatedly, so I won't go into it here, but I'm certainly in agreement that subsidiaries of public institutions should be held accountable under FIPPA.

From Commissioner Denham (page 151):

I do think it's a significant issue. We've certainly written to ministers over time and talked about this in other FIPPA reviews. The bottom line is when public resources are used to operate a subsidiary corporation, then that subsidiary corporation should be subject to the accountability and transparency requirements in FOI and also follow privacy rules.

I think the most substance you will find on this issue is in the OIPC's written submission, which contains discussion of the issue, and the recommendation she made, which I have included below.

From the OIPC written submission (page 13):

There is no sound policy reason as to why corporations or other agencies created by public bodies should not fall under FIPPA

From the OIPC written submission (page 14):

Recommendation 3:

Amend FIPPA to move paragraph (n) of the definition of "local government body" into the definition of "public body" in

Schedule 1, so that entities such as subsidiaries of educational bodies and the BCACP fall within the scope of FIPPA.

Let me know if you have any questions.

Thanks,

-m

Matt Reed
Director, Strategic Privacy
Privacy, Compliance and Training Branch,
Ministry of Finance

250 514-8870
BC logo for sig

From:	Plater, Carmelina MTIC:EX
To:	Reed, Matt MTIC:EX
Subject:	sub corps
Date:	Wednesday, January 27, 2016 9:40:10 AM
Attachments:	2015 OIPC Special Committee Recommendations.xlsx

Here is one more doc that mentions sub corps….lays out some recent analysis and implications on the IPCs recommendation this year….

Carmelina Plater
Sr.Legislation and Policy Advisor
Strategic Policy and Projects
Ministry of Finance

Page 124 to/à Page 130

Withheld pursuant to/removed as

s.13

MINISTRY OF FINANCE
CORPORATE INFORMATION & RECORDS MANAGEMENT
ESTIMATES NOTE

ISSUE: Subsidiary Corporations under the *Freedom of Information and Privacy Act* (FOIPPA)

s.13

CURRENT STATUS:

- s.13
-
-

KEY FACTS REGARDING THE ISSUE:

- On October 20, 2011, the Minister responsible for FOIPPA received a letter from the OIPC asking the ministry to draft amendments to FOIPPA to ensure coverage of subsidiary corporations of local public bodies.
- The Commissioner made this request in response to a 2009 B.C. Supreme Court decision

(Simon Fraser University (SFU) v. British Columbia (Information and Privacy Commissioner), 2009 B.C.SC 1481) which held that FOIPPA did not extend to the records of SFU's subsidiary corporations.

- The 2010 Special Committee that reviewed FOIPPA made a similar, but slightly broader, recommendation to expand the definition of "public body" in Schedule 1 to include any corporation that is created or owned by a public body, including an educational body.
- s.13
- s.13
- s.13
- s.13
- s.13

s.13

2015 OIPC Recommendations to the FOIPPA Special Committee

s.13

Recommendation	New / Previously Recommended by OIPC
1. Add to Part 2 of FIPPA a duty for public bodies to document key actions and decisions based on the definition of government information" in the Information Management Act.	Previously recommended
2. Amend FIPPA to move paragraph (n) of the definition of "local government body" into the definition of "public body" in Schedule I, so that entities such as subsidiaries of educational bodies and the BCACP fall within the scope of FIPPA.	Previously recommended

s.13

Recommendation	New / Previously Recommended by OIPC
3. Add to Part 3 of FIPPA a breach notification and reporting framework which includes: • A definition of a privacy breach: includes the loss of, unauthorized access to or unauthorized collection, use, disclosure or disposal of personal information. • A requirement to notify individuals when their personal information is affected by a known or suspected breach, if the breach could reasonably be expected to cause significant harm to the individual. • A requirement that a public body report to the Commissioner any breach involving personal information under the custody or control of that public body, if the breach or suspected breach could reasonably be expected to cause harm to an individual and/or involves a large number of individuals; • A timing requirement that process of notification and reporting must begin without unreasonable delay once a breach is discovered; • Authority for the Commissioner to order notification to an individual affected by a breach; and • A requirement that public bodies document privacy breaches and decisions about notification and reporting.	Previously recommended

s.13

4. Amend s. 42 of FIPPA to expand the Commissioner's oversight by granting the Commissioner the jurisdiction to review matters or allegations of unauthorized destruction of records. **The Commissioner should have jurisdiction over the unauthorized destruction of records as set out in:** **• any enactment of British Columbia, or** **• set out in a bylaw, resolution or other legal instrument by which a local public body acts or, if a local public body does not have a bylaw, resolution or other legal instrument setting out rules related to the destruction of records, as authorized by the governing body of a local public body.** **The oversight over unauthorized destruction should come with complementary offences and penalties under FIPPA.**	**New**
5. Amend FIPPA to require public bodies to ensure that the name and type of applicant is only disclosed to the individual at the public body that receives an access request on behalf of that public body, while providing for limited exceptions where the applicant is requesting their own personal information or where the name of the applicant is necessary to respond to the request.	**Previously recommended**

s.13

6. Penalties for offences committed by individuals under FIPPA should be raised to be up to a maximum of $50,000 for both general and privacy offences.	New
7. Add a privacy protection offence to s. 74.1 that makes it an offence to collect, use, or disclosure personal information in contravention of Part 3 of FIPPA.	New
8. Add to s. 29 of FIPPA a requirement that public bodies correct personal information when an individual requests that his or her personal information be corrected if the public body is satisfied on reasonable grounds that the request made should be implemented.	New
9. Section 13(1) of FIPPA should be amended to clarify the following: • "advice" and "recommendations" are similar and often interchangeably used terms, rather than sweeping and separate concepts; • "advice" or "recommendations" set out suggested actions for acceptance or rejection during a deliberative process; • the "advice" or "recommendations" does not apply to the facts upon which the advice or recommendation is based; and • the "advice" or "recommendations" does not apply to factual, investigative, or	Previously recommended

background material, for the assessment or analysis of such material, or for professional or technical opinions.	s.13

Other OIPC Recommendations

Recommendation	s.13
10. Amend ss. 71 and 71.1 of FIPPA to require the publication of any categories of records that are established by the head of a public body or the Minister and made available to the public without an access request. This list should include links to relevant information or records.	
11. Add an exception to s. 33.1(1) that states that a public body may disclose personal information inside or outside of Canada, if the information is contained in a non-statutory investigation or fact-finding report commissioned by a public body, where the head of the public body concludes the public interest in disclosure outweighs the privacy interests of any person whose personal information is contained in the report.	
12. Add to FIPPA a requirement that public bodies have a privacy management program that: • designates one or more individuals to be responsible for ensuring that the public body complies with FIPPA; • is tailored to the structure, scale, volume, and sensitivity of the personal information collected by the public body; • includes policies and practices that are developed and followed so that the public body can meet its obligations under FIPPA, and makes policies publicly available; • includes privacy training for employees of the public body; • has a process to respond to complaints that may arise respecting the application of FIPPA; and • is regularly monitored and updated.	
13. Add a de-identification requirement to s. 33.2(l) of FIPPA for any personal information that is disclosed for the purposes of planning or evaluating a program or activity of a public body.	
14. That FIPPA be amended to limit the exemption in s. 3(J)(e) to Part 2 of FIPPA.	

15. Amend the definition for "data-linking" in Schedule 1 of FIPPA to define data-linking as the linking or combining of data sets where the purpose of linking or combining the information is different from the original purpose for which the information in at least one of the data sets that was originally obtained or compiled, and any purposes consistent with that original purpose.	s.13
16. Repeal s. 36.1(2) of FIPPA to remove the exemption of the health care sector from the data-linking oversight provisions of the Act.	
17. Amend Part 6 of FIPPA to require government to list provisions in statutes that prevail over FIPPA in a schedule to the Act, and amend s. 80 of FIPPA to include a review of those provisions as part of the statutory review of the Act.	
18. Amend s. 56 of FIPPA to permit the Commissioner to extend the 90 day time limit to review requests in a manner that is consistent with s. 50(8) of PIPA.	
19. Amend parts 4 and 5 of FIPPA to combine the complaint process and the review and inquiry process into a unitary process for the Commissioner to investigate, review, mediate, inquire into and make orders about complaints respecting decisions under FIPPA or other allegations of non compliance with FIPPA.	
20. Government should enact new comprehensive health information privacy legislation at the earliest opportunity.	
21. Amend section 80 (1) of FIPPA to change the review cycle from 6 years to every 3-4 years.	

Attachment 5 - Past Recommendations of the Special Committee

	Addressed
2004 - 27 - Update the Schedule of Fees in the FOIPP Regulation to reflect the use of electronic media such as CDs and DVDs.	Resolved through legislation
2004 - 01 Change the sensitivity ratings process used in government's corporate request tracking system so that complexity becomes the sole criterion for classifying access requests, and so that the new complexity ratings process protects applicants' identities and treats them equally.	Resolved through policy
2004 - 03 Investigate why the British Columbia Society for the Prevention of Cruelty to Animals was assigned the dual status of a public body and a not-for-profit society and whether there is a case for clarifying or changing its status.	Assessed, no amendments necessary
2004 - 05 Amend the FOIPP Act to require provincial public bodies to adopt schemes approved by the Information and Privacy Commissioner (Commissioner) for the routine disclosure of electronic records.	Resolved in part through legislation
2004 - 06 Amend the FOIPP Act to establish that an applicant who makes a formal access request has the right to anonymity throughout the process.	Resolved through policy
2004 - 07 Amend the FOIPP Act's access request response timelines by giving the Commissioner the authority to grant extensions for rare or unexpected events where the Commissioner considers it fair and reasonable to do so.	Resolved through legislation
2004 - 08 Amend the time period for transferring an access request to another public body so that it is consistent with the time period for responding directly to an access request. Both time periods will start only when a public body has sufficient detail to identify the records and the applicant's authority to request the records.	Resolved through legislation
2004 - 09 Amend the FOIPP Act to authorize public bodies to transfer access requests to any public sector entity that is subject to a federal, provincial or territorial access-to-information statute.	Resolved through legislation

Attachment 5 - Past Recommendations of the Special Committee

2004 - 11 Amend the advice and recommendation exception to indicate these are similar terms that set out suggested actions for acceptance or rejection during the deliberative process, and to limit the information a public body can consider to be advice or recommendations.	Resolved in part through policy
2004 - 13 Amend the FOIPP Act so that it would not apply to records available for purchase by the public and, as a consequence, repeal the access exception for information available for purchase by the public.	Resolved through legislation
2004 - 14 Amend the FOIPP Act so that it would *not* be an unreasonable invasion of privacy to disclose the personal information of a person who has been dead 20 years.	Resolved through legislation
2004 - 15 Amend the FOIPP Act to encourage public bodies to incorporate the use of privacy-enhancing technologies, approved by the Commissioner, into their privacy policies and practices.	Resolved in part through policy
2004 - 16 Amend the disclosure provisions to permit a school board to disclose personal information for archival or historical purposes. This would permit school boards that may not have archives to disclose personal information to a local museum or other such body in order to preserve school memorabilia.	Resolved through legislation
2004 - 18 Amend the Commissioner's powers to permit him to require applicants first to attempt to resolve their complaints and requests for review with the public bodies in a manner that the Commissioner directs.	Resolved through legislation
2004 - 19 Amend the 90 day review period so that it does not include any time taken for referring a matter back to the public body.	Resolved through legislation
2004 - 21 Eliminate the reference to the *Inquiry Act* in the FOIPP Act and instead provide the Commissioner with express powers to order the production of records or things and the attendance of individuals in connection with any investigation, audit or inquiry.	Resolved through legislation
2004 - 22 Amend the FOIPP Act to protect the Commissioner and those acting for or under the direction of the Commissioner from testimonial compulsion.	Resolved through legislation

Attachment 5 - Past Recommendations of the Special Committee

2004 - 23 Provide the Commissioner with the power to order a public body to perform its duty to sever excepted information and to disclose the remainder of the requested records.	Resolved through legislation
2004 - 24 Allow for the enforcement of the Commissioner's orders as orders of the Supreme Court of British Columbia.	Resolved through legislation
2004 - 4 Amend the scope of the FOIPP Act to indicate specifically that records created by or in the custody of a service provider under contract to a public body are under the control of the public body.	Resolved through legislation
2010 - 01 Add a new section 2(3) to acknowledge that information technology plays an important role in achieving the dual purposes of the Act by facilitating the routine disclosure of general information as well as enhancing safeguards for privacy protection.	Resolved through legislation
2010 - 02 Add a new section 2(4) to require that for an infringement of the right to privacy to be lawful, it must be proportional to the public interest that is achieved.	Resolved through policy
2010 - 03 Include the British Columbia Society for the Prevention of Cruelty to Animals by using definition (b) of public body in Schedule 1 that makes provision for adding an "other body" by regulation to Schedule 2; and add the proviso that access rights pertain only to those records that relate to this Society's statutory powers.	Assessed, no amendments necessary
2010 - 05 Amend Section 3 to clarify that records created by or in the custody of a service-provider under contract to a public body are under the control of the public body on whose behalf the contractor provides services.	Resolved through legislation
2010 - 06 Amend section 3(1)(e) by replacing "employees" with "faculty members and teaching support staff" of a post-secondary educational body.	Resolved through legislation

Attachment 5 - Past Recommendations of the Special Committee

2010 - 07 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 Information and Privacy Commissioner for the routine proactive disclosure of electronic records, and to have them operational within a reasonable period of time.	Resolved through legislation
2010 - 08 Amend section 13(2) to require the head of a public body to release on a routine and timely basis the information listed in paragraphs (a) to (n) to the public.	Resolved through policy
2010 - 09 Amend section 9(2) of the Act to require that public bodies provide electronic copies of records to applicants, where the records can reasonably be reproduced in electronic form.	Resolved through legislation
2010 - 10 Amend section 4(1) to establish that an applicant who makes a formal access request has the right to anonymity throughout the entire process.	Resolved through policy
2010 - 11 Amend sections 5 and 9 to allow applicants a right of access to original records if reasonable.	Resolved through legislation
2010 - 12 Amend section 11 to reduce the time allowed for file transfers to ten business days.	s.13
2010 - 13 Make section 14 a mandatory exception, by changing "may refuse" to "must refuse" except when the public body is the client and can choose to waive privilege, or, if the client is a third party, the client agrees to waive privilege.	Not addressed, nor under consideration (Commissioner objected)
2010 - 14 Amend section 14 of the Act to state that decisions on the privileged status of materials when FOI requests are made must be referred to the Supreme Court of British Columbia	Not addressed, nor under consideration (Commissioner objected)
2010 - 15 Amend section 20(3) to provide for immediate release of all requested records if 90 days have elapsed since receiving the applicant's request; and to provide that an access request may be refused if the information will be published according to a statutory schedule.	Resolved through legislation

Attachment 5 - Past Recommendations of the Special Committee

2010 - 16 Amend section 22(2) to state that the personal information of an individual who has been dead for over 20 years is a relevant consideration in determining whether the disclosure of the deceased's personal information would be an unreasonable invasion of personal privacy.	Resolved through legislation
2010 - 17 Amend section 22(3)(h), as follows: "The disclosure could reasonably be expected to reveal the substance of a personal recommendation, or evaluation, character reference, or personnel evaluation, that was supplied in confidence by a third party, or, to reveal the identity of the third party who supplied the reference in confidence." A corresponding amendment would be required to repeal section 22(5).	Resolved through legislation
2010 - 18 Amend section 22(4)(i) by adding "degree, diploma or certificate" granted to the third party by a public body.	Resolved through legislation
2010 - 19 Review section 25(1) in light of the Supreme Court of Canada decision, Grant v. Torstar Corp	Assessed, no amendments necessary
2010 - 20 Amend the Act to allow an individual to consent to the collection, use and disclosure of their personal information by a public body (similar to the *Personal Information Protection Act*).	Resolved through legislation
2010 - 21 Amend the Act to include language confirming a broader approach to research so that applied research into issues, facts, trends, etc for the purpose of program planning and/or evaluation can be undertaken, provided that only de-identified data are used	Resolved in part through legislation
2010 - 23 Appoint a Government Chief Privacy Officer	s.13
2010 - 25 Add a requirement in the Act that privacy impact assessments must be completed at the conceptual, design and implementation phases of an electronic record project. This requirement should apply to health authorities as well as government ministries.	Resolved through legislation
2010 - 26 Amend the Act to reflect the approach taken in the Personal Information Protection Act with respect to the collection of employee personal information.	Resolved through legislation
2010 - 27 Re-examine the protocols regarding sharing health information	Resolved through policy

Attachment 5 - Past Recommendations of the Special Committee

with immediate family members.	s.13
2010 - 28 Amend section 35 of the Act to permit a health care body to disclose de-identified personal health information without the individual's consent for legitimate research purposes.	
2010 - 29 Amend section 42 to explicitly give the Commissioner the power to require public bodies to submit statistical and other information related to their processing of freedom-of-information requests, in a form and manner that the Commissioner considers appropriate.	Resolved through policy
2010 - 32 Amend section 59(2) and add a new section 59(3) to inhibit abuse of the judicial review process by time-limiting the automatic stay of the Commissioner's order.	Resolved through legislation
2010 - 33 Amend section 66 of the Act to include local government bodies in order that local governments have the option of appointing the Chair of the Board or the Mayor of the municipality as the head of the public body with the ability to delegate the duties, power or function to staff.	Resolved through legislation
2010 - 34 Amend section 71 to require public bodies to make available to an individual his or her own personal information free of charge and without an access request, but subject to any access exceptions under the Act	Resolved through legislation
2010 - 35 Review the Schedule of Maximum Fees with an emphasis on meeting the original objectives of the legislation and use the criterion of reasonableness throughout the whole process.	Resolved through regulation

Attachment 5 - Past Recommendations of the Special Committee

Not Addressed	
2004 - 02 Add a new provision stating that the FOIPP Act recognizes that new information technology can play an important role in achieving the FOIPP Act's purposes, particularly with respect to promoting a culture of openness, informal access to information, and in enhancing privacy protection.	Under Consideration
2004 - 10 Develop formal information-sharing agreements with jurisdictions in Canada with the statutory authority to transfer requests to B.C. and encourage other jurisdictions lacking such authority to provide for reciprocal agreements.	Under Consideration
2004 - 12 Amend the FOIPP Act to require public bodies to routinely release the information that is specifically excluded from coverage of the advice and recommendations exception.	Under Consideration
2004 - 17 Amend the FOIPP Act so that the Commissioner can require public bodies to submit statistical and other information related to access requests.	Under Consideration
2004 - 20 Amend the FOIPP Act to combine the separate existing processes for reviewing complaints about public bodies under the FOIPP Act, and for conducting reviews of public bodies' responses to access requests or personal information correction requests. This will create a unified process for the Commissioner to investigate, mediate, inquire into and make orders about complaints and requests for reviews concerning public bodies.	Accepted, amend at next legislative opportunity
2004 - 25 Limit the stay of a Commissioner's order that is under judicial review to 60 days, after which a court may abridge or extend, or impose conditions on, the stay of the order.	Under Consideration
2004 - 26 Amend the FOIPP Act to require public bodies to routinely make available an individuals' personal information free of charge and without an access request, subject to any access exceptions under the FOIPP Act.	Under Consideration

Attachment 5 - Past Recommendations of the Special Committee

2010 - 04 Expand the definition of "public body" in Schedule 1 to include any corporation that is created or owned by a public body, including an educational body.	Under consideration
2010 - 22 Consider holding public consultations on data sharing initiatives	Under Consideration
2010 - 24 Amend the Act to require that data sharing projects for the purpose of research must be subject to ethics review by an arm's length stewardship committee.	Under consideration
2010 - 30 Combine the complaint process and the review and inquiry process - referred to in sections 42(2) and 52(1) respectively - into a unitary process for the Commissioner to investigate, mediate, inquire into and make orders about complaints respecting decisions under the Act and other allegations of non-compliance with the Act.	Accepted, amend at next legislative opportunity
2010 - 31 Amend section 56 to permit the Commissioner to extend the 90-day time limit to review access requests in a manner that is consistent with section 50(8) of the *Personal Information Protection Act*.	s.12,s.13
28 Update the FOIPP Regulation to make it consistent with the equivalent provisions in the Personal Information Protection Act Regulations.	Accepted, amend at next legislative opportunity