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

LEGISLATIVE ASSEMBLY
PROVINCE OF BRITISH COLUMBIA

MAY 2016

May 11, 2016

To the Honourable
Legislative Assembly of the
Province of British Columbia

Honourable Members:

I have the honour to present herewith the Report of the Special Committee to Review the *Freedom of Information and Protection of Privacy Act*.

The Report covers the work of the Committee in the Fourth and Fifth Sessions of the 40th Parliament and was approved unanimously by the Committee.

Respectfully submitted on behalf of the Committee,

Don McRae, MLA
Chair

Table of Contents

Composition of the Committee

Members

Don McRae, MLA	Chair	Comox Valley
Doug Routley, MLA	Deputy Chair	Nanaimo-North Cowichan
Kathy Corrigan, MLA		Burnaby-Deer Lake
David Eby, MLA		Vancouver-Point Grey
Eric Foster, MLA		Vernon-Monashee
Sam Sullivan, MLA		Vancouver-False Creek
Jackie Tegart, MLA		Fraser-Nicola
John Yap, MLA		Richmond-Steveston

Committee Staff

Susan Sourial, Clerk Assistant, Committees and Interparliamentary Relations

Helen Morrison, Committee Research Analyst

Terms of Reference

On February 17, 2016,[1] the Legislative Assembly agreed that a Special Committee be appointed to review the *Freedom of Information and Protection of Privacy Act*, R.S.B.C. 1996, c. 165 pursuant to section 80 of that Act, and that the Special Committee so appointed shall have the powers of a Select Standing Committee and is also empowered:

(a) to appoint of their number one or more subcommittees and to refer to such subcommittees any of the matters referred to the committee and to delegate to the subcommittee all or any of its powers except the power to report directly to the House;

(b) to sit during a period in which the House is adjourned, during the recess after prorogation until the next following Session and during any sitting of the House;

(c) to adjourn from place to place as may be convenient;

(d) to conduct public consultations by any means the committee considers appropriate, including but not limited to public meetings and electronic means; and

(e) to retain personnel as required to assist the committee;

and shall submit a report, including any recommendations respecting the results of the review, to the Legislative Assembly by May 26, 2016; and shall deposit the original of its reports with the Clerk of the Legislative Assembly during a period of adjournment and upon resumption of the sittings of the House, the Chair shall present all reports to the Legislative Assembly.

[1] The Legislative Assembly originally adopted the Committee's Terms of Reference on May 27, 2015, which were renewed on February 17, 2016, for the Fifth Session of the 40th Parliament.

Executive Summary

In May 2015, the Legislative Assembly established a special committee to conduct the fourth statutory review of the *Freedom of Information and Protection of Privacy Act* ("FIPPA") as required by s. 80 of FIPPA. The Special Committee to Review the *Freedom of Information and Protection of Privacy Act* ("the Committee") was briefed by government and the Information and Privacy Commissioner for British Columbia and launched a public consultation process. The Committee heard 24 oral presentations and received 169 written submissions.

The Committee agreed with many of the submissions that, overall, FIPPA is a leading model, both in Canada and internationally, for access to information rights and the protection of informational privacy. The Committee also recognized that specific reforms are needed to address concerns about the freedom of information process and the heightened need for stronger privacy protection in the digital age. The Committee thought that several new provisions should be added to FIPPA, many of which are already in access and privacy laws in other jurisdictions in Canada because of the need to address similar issues.

The Committee made eleven major recommendations covering the following areas:

- measures to enhance proactive disclosure, including a publication scheme;
- a duty to document key decisions and actions of public bodies;
- a cohesive and robust information management framework in government with archiving as a high priority;
- retention of the data sovereignty requirement;
- extending the application of FIPPA to cover subsidiary entities of public bodies;
- changes to timelines and the right to anonymity to support a fair, efficient, and responsive freedom of information process; and
- mandatory notification to affected individuals and reporting to the Information and Privacy Commissioner about significant privacy breaches in order to mitigate risks to privacy.

The Committee made 28 other recommendations in response to submissions received during its consultation process, including with respect to access, privacy, oversight of the Information and Privacy Commissioner, and enforcement. Principal among these are proposed amendments to FIPPA that would:

- require public bodies to have a privacy management program;

- expand the oversight powers of the Information and Privacy Commissioner to include investigations of the destruction of documents contrary to information management rules;
- make the unauthorized destruction of documents with the intention to evade access rights under FIPPA an offence under FIPPA; and
- make the unauthorized collection, use, and disclosure of personal information an offence under FIPPA.

The Committee also recommended that government enact new stand-alone health information privacy legislation.

The Statutory Framework

Modern democracies around the world have public sector access to information and privacy laws. They reflect fundamental democratic values, including openness, transparency, and accountability as well as informational privacy. In Canada, rights created by access to information and privacy laws have been recognized by the courts as quasi-constitutional in nature.

British Columbia's *Freedom of Information and Protection of Privacy Act* ("FIPPA") was passed unanimously by the Legislative Assembly in 1992. Access provisions in Part 2 give information rights to individuals and require public bodies to respond to their requests for information. Protection of privacy measures in Part 3 impose limits on the collection, use, and disclosure of personal information by public bodies and require data security. Parts 4 and 5 of the Act set out an oversight framework that includes the appointment of an Information and Privacy Commissioner as an independent statutory officer of the Legislature with the authority to monitor the administration of FIPPA.

FIPPA applies to some 2,900 public bodies in British Columbia, including ministries, Crown corporations, health authorities, professional regulatory bodies, school boards, municipalities, universities, and municipal police boards.

Pursuant to s. 80 of FIPPA, a special committee of the Legislative Assembly must undertake a comprehensive statutory review of FIPPA at least once every six years, and submit a report to the Legislative Assembly within one year. Previous statutory reviews were conducted in 1998-99, 2004, and 2009-10.

On May 27, 2015, the Legislative Assembly established the Special Committee to Review the *Freedom of Information and Protection of Privacy Act* to conduct the fourth statutory review of FIPPA, and to submit a report to the Legislative Assembly by May 26, 2016. The Committee was re-activated in the Fifth Session of the 40th Parliament on February 17, 2016.

Developments since the 2009-10 Statutory Review

2011 Amendments to FIPPA (Bill 3)

The *Freedom of Information and Protection of Privacy Amendment Act, 2011* (Bill 3) was passed by the Legislative Assembly in October 2011. Among other things, it authorized greater data sharing, including for the purposes of issuance of the BC Services Card, for planning or evaluating government programs, and for common or integrated programs or activities. It expanded oversight by the Information and Privacy Commissioner through mandatory review of privacy impact assessments by her office with respect to common or integrated programs and data-linking initiatives and consultations on an information-sharing code of practice and data linking regulations. The Bill also included new measures in relation to proactive disclosure.

Several amendments recommended by the previous statutory review committee in relation to both access and privacy were implemented. These include a requirement that public bodies provide electronic copies of records to applicants where the records can reasonably be reproduced in electronic form, making the death of an individual for over 20 years a relevant consideration in a determination as to whether disclosure would be an unreasonable invasion of privacy, and allowing an individual to consent to the collection, use, and disclosure of their personal information by a public body.

Access to Information in Government

Government receives 8,000 to 10,000 access requests per year. The cost to government of processing these requests in 2015/16 was estimated at $20 million. This included direct costs to support the operations of government's centralized Information Access Office (an $8 million budget allocation) and indirect costs of processing access requests across central agencies and ministries (an estimated $12 million). The cost to process an average request in 2015/16 was $2,250. In addition, the 2015/16 budget of the Office of the Information and Privacy Commissioner (excluding lobbyist registration) was $5 million.

In a December 16, 2015 statement, government announced that responsibility within government for the Chief Records Officer and information access, policy and operations was being transferred from the Minister of Technology, Innovation and Citizens' Services to the Minister of Finance, and that the transfer would "provide corporate oversight and guidance to all ministries and … begin work to develop service enhancements aimed at improving our duty to assist freedom of information applicants."

During the past six years, the Information and Privacy Commissioner has released five reports regarding government's responsiveness to access requests. These include evaluations of the timeliness of government's responses, as well as investigations of complaints regarding an increase in the number of instances where there were no responsive records and the unauthorized destruction of records.

In these reports, the Information and Privacy Commissioner recommended improvements to government's freedom of information ("FOI") process and amendments to FIPPA. The recommendations include specific measures that would assist applicants and facilitate greater responsiveness, routine proactive disclosure of calendars of senior executives, training for government employees, a duty to document within FIPPA, and independent oversight of information management requirements.

Government's Open Government Initiative

In 2011, government announced an open government (or proactive disclosure) initiative with the following three components: open information, a disclosure log, and open data.

Under the open information policy, travel expenses of ministers and deputy ministers are posted on government's Open Information website one month after the expenses are claimed. Separate amounts are shown for in-province flights, other in-province travel, out-of-province travel, out-of-country travel, monthly total, and fiscal year-to-date total. The information can be downloaded in PDF format.

Other documents that have been posted on the Open Information website include documents related to the Review of the Draft Multicultural Strategic Outreach Plan which were posted in June 2013.

Government's disclosure log can be accessed through the Open Information website by clicking on "Find Information Releases." With some exceptions, government's responses to access requests are posted together with a summary of the applicant's request and its response letter. Among the exceptions are records that contain personal information.

In terms of open data, government's DataBC program is responsible for publishing dataset information from ministries on a DataBC website. There are currently over 2,000 datasets on the DataBC site. Ministries are responsible for de-identification and privacy assessments of their data before submitting it as open data. Users can search the data by ministry or by subject matter.

Privacy Breaches

Privacy breaches in today's digital environments have the potential to be much more far-reaching and damaging than in the paper-based world of what is practically a bygone era. Public bodies are storing massive amounts of data in mega databases that are vulnerable to hackers, snooping, and other unauthorized disclosures. Portable storage devices for data can be easily lost or stolen. For these reasons, compliance with privacy protective obligations under FIPPA is becoming increasingly important. Compliance challenges are also greater given that the vast quantities of data are being collected in an environment of rapidly evolving technology, new security threats and risks, and high employee turnover rates.

Since the last statutory review, there have been a number of significant privacy breaches within the public sector. The following examples are illustrative of their nature and scope:

- the loss of a portable hard drive containing the personal information of 3.4 million British Columbia and Yukon teachers and students;
- snooping of the personal information of 112 individuals within an electronic health record system;
- personal information on portable storage devices disclosed externally without proper authority to a contracted service provider and researchers;
- the theft of a portable storage device containing personal identity and financial information of almost 12,000 current and former employees; and
- data crossover of personal identity and financial information in customer accounts on an online gaming platform.

Among the lessons learned from these occurrences is the critical importance of public bodies having policies and procedures in place, that are up to date and well understood by every employee, on how to prevent and mitigate privacy breaches, when to notify affected individuals, and how to do so appropriately. British Columbians expect public bodies to have a strong commitment to, and a proper investment in, privacy protection throughout every level of the organization. Preventable privacy breaches are symptomatic of a failure on the part of a public body to guard personal information adequately.

Recent Legislative Reviews in Other Canadian Jurisdictions

Three reports on the results of reviews of other access and privacy laws in Canada were published in 2015. They are the report of an independent statutory review committee in

Newfoundland and Labrador, a special report of the Information Commissioner of Canada, and a position paper of the Government of Quebec.

Newfoundland and Labrador Review (2014-15)

A committee was appointed by the Premier of Newfoundland and Labrador in March 2014 to conduct an independent statutory review of the Newfoundland and Labrador *Access to Information and Protection of Privacy Act* (ATIPPA). This review was conducted two years ahead of the mandatory 5-year review because of widely expressed concern about amendments made to ATIPPA in 2012 (Bill 29) which resulted in a lack of confidence in the integrity of the access to information system.

The three members of the 2014 Review Committee were Clyde Wells, Q.C., (lawyer, former Chief Justice, and former Premier), Jennifer Stoddart (former Privacy Commissioner of Canada), and Doug Letto (journalist). The 2014 Review Committee presented a lengthy and comprehensive report to government in March 2015. The 480-page report includes a discussion of the stature of access and privacy laws, summaries of presentations made during the public consultation process, comparative information regarding access and privacy laws elsewhere, analyses of possible reforms, and a draft bill.

The 2014 Review Committee recommended a major overhaul of ATIPPA and made 96 specific recommendations. In April 2015, a proposed new statute based on its recommendations was introduced in the House of Assembly of Newfoundland and Labrador. It received Royal Assent and came into force in June 2015 as the *Access to Information and Protection of Privacy Act, 2015*. The new law has been ranked as the best access and privacy law in Canada by the Centre for Law and Democracy (FIPPA is ranked second).

Recommendations made by the 2014 Review Committee include the following:

- Mandatory breach notification
    - Public bodies should be required to notify the Commissioner of privacy breaches and notify affected individuals where there is a risk of significant harm created by the privacy breach.
- Duty to document
    - A duty to document decisions should be added to information management legislation.

- Proactive disclosure and Open Government / Open Data
    - The definition of "records" should include datasets and other machine readable records and there should be a requirement for datasets to be released in a re-usable format.
    - Public bodies should be required to publish information on a proactive basis in accordance with a model publication scheme.
- Powers of the Information and Privacy Commissioner
    - The Office of the Information and Privacy Commissioner should remain as an ombuds oversight model.
- The Act should provide for a banking system in the Commissioner's office where there are multiple complaints by one individual.
- The Commissioner's powers should be expanded to explicitly include authority to:
    - monitor or audit compliance with the duty to document,
    - develop a model publication scheme for public bodies, and
    - review proposed bills for access and privacy implications.
- Offence provision
    - The offence provision should be strengthened, including making it an offence for a person to destroy a record, erase information in a record, and alter/falsify/conceal a record or directing another person to do so.
- Provisions that prevail over FIPPA
    - A review of legislative provisions that prevail over ATIPPA must be part of a statutory review.

Special Report of the Information Commissioner of Canada (2015)

In March 2015, the Information Commissioner of Canada, Suzanne Legault, submitted a special report to Parliament proposing a comprehensive modernization of the federal *Access to Information Act***.** The 85 recommendations contained in her 104-page report titled, *Striking the Right Balance for Transparency*, are based on the experience of her office, as well as comparisons to leading access to information provincial, territorial, and international laws. Many of the recommendations emulate existing provisions of FIPPA, particularly with respect to the oversight authority of the Information and Privacy Commissioner for British Columbia. Other proposals include establishing a duty to document; eliminating all fees related to access requests; the inclusion of a general public interest override; open information requirements; and new offence provisions.

Government of Quebec Position Paper (2015)

A 190-page position paper titled, *Government policy directions for a more transparent government, respectful of a person's right to privacy and the protection of personal information (Orientations Gouvernementales pour un Gouvernement Plus Transparent, dans le Respect du Droit à la Vie Privée et la Protection des Renseignements Personnels*), outlines the Quebec government's intention to reform access and privacy law in order to promote a culture of transparency, and strengthen access to information requirements. Among other things, government would require more documents and more information on government activities and expenditures to be made public and datasets to be released in a format that permits re-use. Government also wishes to adopt a new organizational model for the Commissioner's office where judicial rulings in response to requests for review of decisions of public bodies would be handled by another body such as the Administrative Tribunal of Quebec. The Commissioner's office would retain responsibility for monitoring, mediation, advocacy, and providing information. The National Assembly of Quebec's Committee on Institutions held general consultations and public hearings on the position paper in the fall of 2015.

The Consultation Process

The Committee met on May 28, 2015 and July 16, 2015 to plan and organize its work. The Committee agreed to request initial briefings from government and the Information and Privacy Commissioner for British Columbia on the history and administration of FIPPA, before launching public consultations on the effectiveness of FIPPA.

Initial Briefings

Ministry of Technology, Innovation and Citizens' Services

On July 16, 2015, the Ministry of Technology, Innovation and Citizens' Services provided the Committee with an overview of government's activities with respect to the application of FIPPA.

The Ministry provided the following statistical information regarding access requests to government:

- government receives 8,000 to 10,000 requests per year (two to three times as many requests per capita as Ontario);
- the on-time rate of government responses to requests increased to 79 percent in 2014-2015, up from 74 percent in 2013-2014;
- the percentage of no responsive records in government fell from 25 percent in 2012-2013 to 17 percent in 2014-2015;
- approximately one to two percent of all requests made to public bodies result in a request for a review by the Information and Privacy Commissioner;
- the number of general requests made to government has increased more than twofold since 2008-09, when government centralized its FOI services;
- in 2014-2015, 99 percent of all complaints received by the Office of the Information and Privacy Commissioner were resolved without hearing or inquiry;
- 70 percent of the general requests received by government over the past two years were from political parties and media applicants; and
- fees were paid by an applicant in less than two percent of requests made to government.

Government recovers only a very limited portion of the costs associated with processing access requests. BC does not have an application fee such as exists in other jurisdictions, but public bodies may charge fees for searching for records, preparing records, and for shipping (except in the case of requests from individuals for their own personal information). Fees can be waived by a public body.

The Ministry provided the Committee with a document on the disposition of the 35 recommendations made by the previous committee in 2010. The Committee was advised that 16 recommendations were addressed in the amendments made in 2011, one was addressed in an amendment to the regulation, six were fully or partly addressed through policy, seven were reviewed and no amendments were deemed necessary, one will be implemented when a proposed amendment receives approval to proceed, and four remain under consideration.

Information and Privacy Commissioner

In her presentation to the Committee on July 21, 2015, the Information and Privacy Commissioner discussed FIPPA in the global context, and external trends affecting access and privacy.

She noted that access to information laws exist in over 100 countries, and 109 jurisdictions have privacy or data protection laws. External trends include the rapid acceleration in the use of technology and law reform in the areas of accountability and effective oversight. With respect to the use of technology, the Commissioner highlighted its impact on the health sector, and submitted that because health information is increasingly part of an integrated system that operates across the public and the private sectors, specific rules are needed for personal health information.

In terms of law reform and accountability, the Commissioner outlined elements of a framework that would include privacy training, privacy policies, transparency reporting for disclosures to law enforcement, audit controls to monitor access, data breach response plans, and mandatory breach notification. The Commissioner also applied the principle of accountability to access to information and said that it means proactive disclosure, a duty to document key actions and decisions of government, proper records management and archiving regimes, and ensuring that information is not deleted or destroyed in an unauthorized manner. New measures in relation to effective oversight could include having legislative authority to ensure proper information management systems are in place and providing administrative penalties and sanctions for deliberate destruction of records.

The Commissioner identified trust, transparency, and accountability as values that should continue to underpin any recommended changes the Committee may make. In the Commissioner's view, the current law is a solid framework.

The Commissioner was asked about the delay in implementation of a previous recommendation made in the third statutory review regarding the application of FIPPA to subsidiary corporations of educational bodies. She expressed concern about this accountability gap in FIPPA, and advised that she has written to the responsible ministers twice asking for an update on government's consultation process in relation to the recommendation. In response to Members' questions about possible barriers to access to data for health research, the Commissioner indicated that she has proposed a secure research platform so that health information may be accessed more readily by public interest researchers.

Briefings on the Loukidelis Report

On March 16, 2016, the Committee received briefings from officials in the Ministry of Finance and the Information and Privacy Commissioner on government's response to recommendations made to government in December 2015 by David Loukidelis, Q.C.,(former Information and Privacy Commissioner), regarding implementation of Investigation Report F15-03.

Investigation Report F15-03, titled *Access Denied: Record Retention Practices of the Government of British Columbia*, was released by the Information and Privacy Commissioner in October 2015. In the report, the Information and Privacy Commissioner made findings in relation to three specific complaint investigations involving political staff in three executive branch offices and recommended amendments to FIPPA, including adding a duty to document and independent oversight of government information management.

In his report, Mr. Loukidelis made 27 recommendations to government for reform and improvement of its information management practices. These include improvements to the FOI process, measures to enhance training for political staff in ministers' offices and staff in the Premier's office, updating government's transitory records policy, ensuring early compliance with the new *Information Management Act*, mandatory training for public servants on records management, and legislative amendments for a duty to document and the unauthorized destruction of records.

In her presentation to the Committee, government's Chief Records Officer indicated that government is taking action on all 27 recommendations in the Loukidelis report. It is

revitalizing the service culture in regard to FOI processes in accordance with the following key principles: transparency, accountability, subject matter expertise, timeliness, fairness, and improved service orientation. Specific commitments include improving timeliness in responding to access requests, reducing the number of "no records" responses, and advancing the duty to assist. Government is considering significant changes to FOI processes in minister's offices, including designating a contact within each deputy minister's office who will be responsible for coordinating and overseeing searches for records and for supporting records management practices. Government has a compliance program that includes mandatory training for all public servants. It is emphasizing duty to document principles in updating records management policies.

In her presentation, the Information and Privacy Commissioner stated that the Loukidelis report provides a clear path to implementing key aspects of her recommendations in Investigation Report F15-03. These include recommendations to create a duty to document, independent oversight over the unauthorized destruction of records, and an offence for the destruction of records.

Privacy and Access Conference

The Chair and Deputy Chair attended a privacy and access conference hosted by the Information and Privacy Commissioner, titled *Privacy and Access 20/20: The Future of Privacy*, from November 12 to 13, 2015, in Vancouver. Conference sessions focused on emerging privacy issues and the nature of the discourse among regulators, the public sector, organizations, and privacy experts about the risks to privacy they present and how they should be addressed. Many areas of concern raised during the Committee's public consultations were discussed at the conference, including health privacy, big data, and online digital identities. A final session on the future of privacy highlighted the need to ensure that the Committee's recommendations are forward-looking, and that they remain relevant in the face of rapidly evolving technology.

Public Consultation

On July 25, 2015, the Committee issued a province-wide media release announcing that the Committee was conducting a public consultation process as part of its review of FIPPA and inviting oral presentations and written submissions. A Committee webpage was created with information on how to participate in the public consultations. Participants in previous reviews and experts were contacted to invite them to make submissions. Ads were placed in newspapers across the province in September 2015 inviting individual British Columbians to participate.

The Committee held public hearings in Vancouver and Victoria on October 16, 2015, November 9, 2015, and November 18, 2015, with presentations from a total of 24 public bodies, advocacy groups, stakeholders, and individual citizens. A further 169 written submissions were received. The names of the 193 individuals and organizations that presented or provided a written submission are listed in Appendix A.

On March 8, 2016, the Information and Privacy Commissioner provided the Committee with a written response to recommendations the Committee had received during its consultations.

During its public consultation process, the Committee received many thoughtful and insightful recommendations to modernize and improve the effectiveness of FIPPA. Some of these came from individuals and organizations who had concerns with how public bodies fulfilled, or failed to fulfill, their obligations to respond to access requests. The Committee also heard from public bodies who were experiencing difficulties in responding to access requests and/or in complying with the privacy protective provisions of FIPPA. Some submissions reflected different perspectives on whether FIPPA is achieving its public policy goals. A number of submissions were prompted by recommendations in the Information and Privacy Commissioner's October 2015 investigation report (Investigation Report F15-03).

Members of the Committee wish to thank all those who participated in its consultation process. The experiences, expertise, and advice shared with the Committee were invaluable and greatly assisted the Committee in its work. The Committee was impressed with the quality and range of recommendations it was asked to consider, and is very grateful to have had that input as a foundation for its deliberations and recommendations.

The Committee undertook deliberations respecting its statutory review of FIPPA in March, April, and May 2016. On May 3, 2016, the Committee adopted its report.

Meeting Schedule

May 28, 2015	Organization meeting
July 16, 2015	Briefing and Planning
July 21, 2015	Briefing
October 16, 2015	Public hearing, Vancouver
November 9, 2015	Public hearing, Vancouver

November 18, 2015	Public hearing, Victoria
February 24, 2016	Organization meeting
March 2, 2016	Deliberations
March 10, 2016	Deliberations
March 16, 2016	Briefing
March 24, 2016	Deliberations
April 5, 2016	Deliberations
April 13, 2016	Deliberations
April 21, 2016	Deliberations
April 27, 2016	Deliberations
May 3, 2016	Adoption of Report

Conclusions and Recommendations

Key Principles

To guide its deliberations, the Committee adopted the following key principles:

- The routine proactive disclosure of records supports the underlying principles and objectives of FIPPA, namely openness, transparency, and accountability.
- Solid information management practices are essential for good governance and foundational to the right of citizens to access public sector information.
- The personal information of British Columbians must continue to be protected in the face of technological change.
- FIPPA should apply broadly to the whole of the public sector.
- The FOI process should be user-friendly, fair, efficient, and responsive.
- Citizens must be protected from unauthorized disclosures of their personal information.

Main Findings

The Committee's main findings are based on the presentations and submissions the Committee received during its public consultation process. They are organized under several broad themes:

- The Committee agreed that proactive disclosure is preferable to the FOI process because it avoids the delays and costs involved in making and responding to access requests. It promotes openness and transparency, keeps the public informed about the decisions and actions of public bodies, and enhances public trust and confidence in the public sector.
- The Committee considered that a duty to document and proper archiving are critical aspects of information management. They are needed for good governance, openness, and transparency. There should be legal and policy requirements within public bodies with respect to each.
- The Committee concluded that data sovereignty is important in order for personal information to be properly protected under Canadian law. While the Committee recognized that public bodies may wish to take advantage of the latest advances in technology, including cloud-based solutions, those solutions are becoming

increasingly available in Canada and they should be relied upon exclusively in order to protect the personal information of British Columbians.

- The Committee maintained that any board, committee, commission, panel, agency or corporation that is created or owned by a public body, and all the members or officers of which are appointed or chosen by or under the authority of that public body, should be subject to FIPPA.
- The FOI process is functioning fairly well but the Committee heard concerns with respect to delays in receiving responses to access requests. The Committee thought that the FOI process could be improved by reducing the timelines in which public bodies must respond to access requests and by protecting the anonymity of applicants.
- The Committee accepted that mandatory breach notification and reporting is best practice, and is in the public interest. It helps to mitigate the risks to British Columbians in the event of a privacy breach, and prevent future ones from occurring.

Major Recommendations

The Committee identified the following issues as being significant in the context of its review:

- Proactive disclosure;
- Duty to document;
- Information management in government;
- Data sovereignty;
- The application of FIPPA to subsidiary corporations and other entities;
- The FOI process, including timelines to respond to access requests, and anonymity of applicants; and
- Mandatory breach notification.

Major Recommendations

Proactive Disclosure (Open Government)

The process of making and responding to an access request can be costly and time-consuming for both individuals and public bodies. Right to know advocates prefer open government initiatives where information is pushed out on a proactive basis, in a timely manner, and as a matter of course, rather than only in response to an access request. The Committee received a number of recommendations with respect to proactive disclosure requirements in FIPPA.

Laura Millar, an information, records and archives consultant, made the case for a greater emphasis on proactive disclosure in her testimony before the Committee on November 9, 2015:

> Why not routinely make available as much evidence as possible rather than wait for the public to seek specific records through a limited routine-release policy and an increasingly and sometimes unnecessarily backlogged regime of access only when requested?

As she went on to state, "Open government can save time and money as well as improve trust in government if the processes for creating records in the first place are designed to support both accountability and access."

The Committee believes all public bodies should view their information responsibilities in that light. Open and easy access to records and archives should be the norm. In principle, public bodies should be proactively disclosing records whenever disclosure is in the public interest. To the extent possible, documents should be created and structured in such a way that they can be proactively released, either in whole or in part, on a routine basis. Records for proactive disclosure should include datasets and other machine readable records and there should be a requirement for datasets to be released in a re-usable format.

Strengthen Public Interest Disclosure (s. 25)

Section 25 of FIPPA requires public bodies to disclose to the public, to an affected group of people, or to an applicant, information about a risk of significant harm to the environment, or to the health or safety of the public or a group of people or information the disclosure of which is, for any other reason, clearly in the public interest.

This disclosure is mandatory and overrides the ability of a public body to withhold information based on exceptions from disclosure that might otherwise apply. This public interest override provision has been interpreted to require some degree of temporal urgency to the risk because of the requirement to disclose the information "without delay."

The BC Freedom of Information and Privacy Association and Stanley Tromp advocated removing the requirement of temporal urgency. The BC Civil Liberties Association suggested that a clarifying amendment should be inserted to the effect that the disclosure obligation does not only pertain to situations of emergency, but to any situation in which the disclosure of the information is, for any reason, clearly in the public interest.

The Environmental Law Centre of the University of Victoria proposed a number of amendments that would strengthen the public interest disclosure requirement in s. 25 of FIPPA. They are as follows:

(a) Explicitly require public bodies to proactively disclose information whenever a disinterested and reasonable observer would conclude that disclosure is in the public interest and include two more categories of public interest information (information about a topic inviting public attention, or about which the public has a substantial concern, or that promotes government accountability);

(b) Require proactive disclosure of specific categories and classes of records;

(c) Require the proactive disclosure of environmental information; and

(d) Require that proactively released information be posted online.

The Environmental Law Centre also suggested that government consider making certain policy information a category of records that must be proactively disclosed and permitting the minister to prescribe additional categories or records of information that must be proactively disclosed.

The Committee considered the recommendation made with respect to s. 25 by the previous statutory review committee in 2010. The recommendation was to review s. 25(1) in light of the Supreme Court of Canada decision in *Grant* v. *Torstar Corp* [2009] 3 SCR. In that 2009 defamation case, the Supreme Court held that the law of defamation should be modified to recognize a defense of responsible communication on matters of public interest. Chief Justice McLachlin, writing for the majority, stated that for a given subject matter to be considered as being in the public interest, "It is enough that some segment of the community would have a genuine interest in receiving information on the subject."

The Committee felt that this broader interpretation of the public interest may not be appropriate in terms of the public interest override in s. 25(1). It is, however, an appropriate standard in terms of proactive disclosure generally where exceptions to disclosure could be applied when necessary for good governance and for the protection of personal information.

The Committee concluded that it would be in the public interest to remove the requirement of temporal urgency in s. 25 to require more public interest disclosures. Public bodies should be required to proactively disclose any information about a significant risk of harm to the environment or health or safety, even in non-urgent situations.

Expand Proactive Disclosure Requirements (ss. 13, 71 and 71.1)

Section 71 of FIPPA requires public bodies to establish categories of records in their custody or control that must be made available to the public on a proactive basis. With limited exceptions, a category of records must not contain personal information. Section 71.1 of FIPPA permits the minister responsible for FIPPA to establish categories of records that are in the custody or control of ministries.

The Information and Privacy Commissioner recommended that public bodies and ministries be required to publish a list of the categories of records they establish under this provision, with links to the relevant information or records. This would achieve greater transparency in the implementation of ss. 71 and 71.1.

The Environmental Law Centre of the University of Victoria had a number of recommendations in relation to categories of records. It suggested establishing a category for environmental compliance orders, authorizations, convictions, contraventions, penalties and assessments; environmental quality reports; inspection reports; and penalties under all administrative schemes; contracts over $10,000; final audit reports; and budget and expenditure information. It also submitted that s. 71 should be amended so that it more closely matches the publication scheme requirement in the UK, and requires that the lists be produced and posted within a legislated timeframe.

Both the Canadian Centre for Policy Alternatives and the Canadian Union of Public Employees ("CUPE") BC Division recommended the proactive disclosure of calendar information because of the high volume of requests for it. They endorsed a recommendation previously made by the Information and Privacy Commissioner regarding this in a 2014 investigation report about the timeliness of government's responses to access requests. Their position is that government should develop a system to proactively disclose calendar information of ministers and senior executives.

The Regional District of Kootenay thought that there should be a list of classes of information that all public bodies should proactively disclose to ensure consistency. The City of Surrey recommended defining "proactively disclose" to mean posting on the website of the public body.

Both the Environmental Law Centre and CUPE BC Division maintained that FIPPA should not only mandate disclosure but proactive disclosure of the types of records enumerated in s. 13(2)(a)to (n) of FIPPA. That section mandates the disclosure of certain types of records, including factual material, a public opinion poll, a statistical survey, and a final audit.

In terms of proactive disclosure, government stated in its written submission that the minister has not officially issued a direction under s. 71.1 of FIPPA but that there are categories of government information currently designated for proactive disclosure by policy. Government acknowledged that transparency could be enhanced by formalizing existing proactive releases with a minister's designation and advised that as government re-initiates its proactive disclosure efforts, and designates new categories of information for proactive disclosure the Committee can expect to see the minister use their direction-making authority to formalize the requirement to release information on a proactive basis. The directions will be published on government's Open Information site.

In her presentation to the Committee on March 16, 2016, the Chief Records Officer advised that government is considering a number of options in terms of proactive release, including purchase card information; deputy ministers' and ministers' calendars; government contract information; and direct-award summaries. A deputy ministers committee is also considering other opportunities for open government.

Two previous statutory review committees made the following recommendation in relation to proactive disclosure and s. 13(2):

> 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.

Government advised the Committee during its review that it was addressing this recommendation through a change to its policy and procedures manual and to its FOI training to make sure that public bodies understand that exceptions to disclosure would still need to be applied.

The Committee was not convinced that this is the best approach. A mandated publication scheme, with the records listed in s. 13(2)(a) to (n) as a starting point, should be added to FIPPA in order to effect a cultural shift. Proactive disclosure on websites in accordance with a

standard publication scheme should be prioritized as the principal mechanism by which public bodies provide access to information. The Information and Privacy Commissioner should be consulted with respect to the type of records that should be included in the publication scheme.

Members were also in favour of government disclosing calendar information of ministers and senior officials because of the volume of access requests for that information, and previous recommendations made by the Information and Privacy Commissioner in relation to calendar information.

Recommendation

The Committee recommends to the Legislative Assembly that the provincial government:

1. Amend FIPPA and initiate proactive disclosure strategies that reflect the principle that information that is in the public interest should be proactively disclosed, subject to certain limited and discretionary exceptions that are necessary for good governance and the protection of personal information. Among other things, this could be accomplished by:

    - strengthening s. 25(1) to remove the requirement of temporal urgency;
    - establishing a publication scheme that would apply to all public bodies, that includes mandatory proactive disclosure of those records listed in s. 13(2)(a) to (n); and
    - developing a system within government to proactively disclose the calendar information of ministers and other senior officials that would be disclosed in response to an access request.

Duty to Document

The "duty to document" was raised by both government and the Information and Privacy Commissioner in their submissions to the Committee. It was also a recommendation made by the Information and Privacy Commissioner in her October 22, 2015 investigation report *Access Denied: Record Retention and Disposal Practices of the Government of British Columbia* (Investigation Report F15-03).

Recommendation 11 in Investigation Report F15-03 reads as follows:

> 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.

In her November 18, 2015 written submission to the Committee, the Information and Privacy Commissioner stated that in investigation reports of her office, including Investigation Report F15-03, she has recommended that government adopt a duty to document to demonstrate its commitment to public accountability, in order to preserve the historical legacy of government decisions, and as a key records management component of proactive disclosure programs.

The duty to document was also recommended in a number of other submissions to the Committee. The BC Freedom of Information and Privacy Association, along with other public interest advocacy organizations, unions, and individuals recommended that a duty to document be added to FIPPA so that there are records of decisions and actions of public bodies that may be released in response to access requests.

In his December 2015 report to government, Mr. Loukidelis encouraged government to consider the duty to document after a period of careful study. He suggested that government adopt a risk-based approach, with the nature and significance of decisions, actions, and transactions being used to determine which records have to be created and in what manner.

In its submission to the Committee, the Canadian Bar Association agreed that the issue merits careful study as well as consultations prior to being implemented within government and in public bodies. Questions that would need to be answered include whether the duty should be embedded in legislation and/or policy that deals with information management more generally, and what are the most appropriate consequences for non-compliance.

Submissions to the Committee stressed that solid information management practices are the foundation for access to information. As stated by the Regional District of Kootenay in its submission, "Complete and timely responses to freedom of information requests are

dependent on proper records management practices." The creation of a record is the first critical piece in the capture of information. As the BC Freedom of Information and Privacy Association said in its submission, "There can be no public access to records if records are not created." Records must be created, in the format requested and in machine-readable format, retained, and be retrievable in order for public bodies to be in a position to respond appropriately to access requests.

While information management is essential to the exercise of access rights, it is also essential for a number of other reasons. In his report, Mr. Loukidelis explained the linkage as follows:

> …while information management and freedom of information share common ground they are not the same thing. Good information management rules and practices can foster and support openness and accountability through freedom of information laws, but freedom of information is not – and should not be – the sole aims of records and information management. Put another way, while good records management laws and practices can enhance the functioning of freedom of information laws, that is not, and should not be the sole objective of records and information management.

Records and information laws, policies and practices serve a variety of other important public interest objectives. These include ensuring that the administration of public affairs is in accordance with the law, enhancing the quality and efficiency of public administration, supporting prudent operation of institutions, protecting the legal interests of institutions and the legal rights of citizens, and preserving the historical record. While accountability, an objective of freedom of information, is linked with many of these public interest objectives, accountability does not exhaust the public interest in good records and information management.

Later in his report, he enumerated the following significant risks raised by a failure to keep adequate records:

1. Diminishment or elimination of accountability of elected or appointed officials for their actions and decisions

2. Reduced openness and transparency of government activities, notably through freedom of information requests

3. Harm to sound management and administration of government due to failure to document processes, deliberations and actions (the risk of unrecorded or lost corporate knowledge, experience and learning from mistakes and successes)

4. Litigation risk flowing from government not being able to rely on proper documentation to demonstrate lawful actions and decisions, unnecessarily exposing it to damages and judicial censure

5. Government not being able to rely on proper documentation in response to internal or external audits, exposing government to censure by auditors

6. Loss to the historical record because documents do not exist that have archival and historical importance (with links to the immediately preceding risk)

7. Loss of public confidence in government over time due to the perception that the absence of documentation reflects a deliberate tactic to hide, among other things, wrongdoing (including corruption or favouritism)

Thus, solid information management is not only foundational to freedom of information, but also to sound public administration within a democratic system of government.

There are existing policy and legislative requirements regarding recordkeeping within government. Pursuant to section 12.3.3, Part III of the Core Policy and Procedures Manual, government policy is to create and retain a full and accurate record documenting decisions and actions. Government provided the Committee with a document that sets out provisions in 419 different statutes that contain at least one authority to create a record. For example, the *Budget Transparency and Accountability Act* requires the preparation of the main estimates for a fiscal year and specifies the information they must include; the *Mines Act* requires the Chief Inspector to publish an annual report; and the *Regulatory Reporting Act* requires the minister to publish a report that includes information required by regulations. Many of the statutes listed in the document do not impose obligations in relation to record keeping within government, but rather within municipalities, professional regulatory bodies, or strata corporations.

It would appear that these provisions requiring the creation of specific types of records, while important, do not amount to a duty to document. Although they may require certain reports or other documentation to be prepared for certain purposes, and in most cases, made publicly available, they do not impose a general obligation to create a record of key government decisions or actions.

A statutory duty to document does not currently exist in Canada. It was considered during the Newfoundland and Labrador review and the independent committee recommended that government take the necessary steps to impose a duty to document, and that the proper legislation to express that duty would be the information management statute and not the access and privacy law. There are precedents for a duty to document in information

management statutes in New Zealand (the *Public Records Act*) and in New South Wales (*State Records Act*).

In her written submission, the Commissioner indicated that she would prefer that a duty to document be added to FIPPA rather than to the *Information Management Act*:

> While I have previously stated that a duty to document could be placed in information management legislation there are compelling reasons why FIPPA should contain this requirement. The IMA only applies to ministries and designated government agencies whereas FIPPA applies to all public bodies. Further, there is an integral connection between the duty to document and access rights. Last, FIPPA contains the oversight framework that is needed to ensure that the duty to create and retain records has the appropriate oversight.

In its written submission to the Committee dated March 16, 2016, government said that it is considering the implications of adding a broadly-stated, legislative "duty to document" in addition to the existing policy requirements and other legislative requirements to create records. In its view, given the direction other jurisdictions in Canada and globally have taken around implementing a "duty to document," FIPPA may not be the appropriate legislation in which to add such a duty. It may be more appropriate and consistent to add this duty to information management legislation. Government's position is to "consider adding a broadly-worded, legislated "duty to document" to the *Information Management Act*, with the details to be implemented through policy."

British Columbia's new *Information Management Act* applies to ministries, a government agency designated as a government body by regulation and the courts. It does not apply to local governments. A "government agency" is defined as follows:

> "government agency" means an association board, commission, corporation or other body, whether incorporated or unincorporated, if
>
> (a) the body is an agent of the government,
>
> (b) in the case of a corporation with issued voting shares, the government owns directly or indirectly, more than 50% of the issued voting shares of the corporation, or
>
> (c) a majority of the members of the body or of its board of directors or board of management are one or both of the following:

i. appointed by the Lieutenant Governor in Council, by a minister or by an Act

ii. ministers or public officers acting as minister or public officers.

Members discussed the need for a duty to document key government actions and decisions and considered the precedents in Australia and New Zealand where it is a statutory requirement in information management law. In the Committee's view it is important that the duty be imposed on all public bodies, including local governments. It therefore accepted the recommendation of the Information and Privacy Commissioner that the duty to document should be added to FIPPA, rather than to the *Information Management Act*, because of the breadth of its coverage.

Recommendation

The Committee recommends to the Legislative Assembly that the provincial government:

2. Add a duty to document to FIPPA.

Information Management in Government

The *Information Management Act*, passed by the Legislative Assembly in May 2015, repealed and replaced an antiquated *Document Disposal Act*, and set out new rules for record keeping within government. It authorizes the Chief Records Officer to approve information schedules for the disposal and holding of government information. Government information to which an information schedule applies must be held, transferred, archived, or disposed of, in accordance with the information schedule. Government information is defined as including, among other things, 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 body, and information that documents or supports the government body's organization, policies, procedures, transactions, or operations.

With respect to court information, the Deputy Attorney General and the Chief Judge or Chief Justice of a court may approve a court information schedule and court information must be held, transferred, archived or disposed of in accordance with the court information schedule.

The Act provides that the minister responsible may establish an information management advisory committee to advise the Chief Records Officer in relation to the approval of information schedules applying to a class of government information.

When the Chief Records Officer appeared before the Committee on March 16, 2016, she indicated that the most important thing the *Information Management Act* will do is that it will allow government to be more adaptive and more flexible, respond to new needs around information management and bring those up to date so that the public service at large has very clear direction around what records they should be developing and retaining. She also stated that government is now looking at information as a unified whole over the life cycle of records rather than in the siloed and piecemeal approach it had before.

In her presentation to the Committee, Laura Miller articulated very well what should be the overarching vision and goals for information management in government:

> My vision is that I will live in an enlightened, civilized society, one that is democratic, respectful and self-aware. For my society to be civilized, democratic, respectful and self-aware it needs a memory, a collective consciousness born out of unencumbered access to the evidence of the communications, actions and transactions of its members, from the government to the governed, from formal institutions to people on the street.

> In the society of my dreams, my government recognizes that open and easy access to records and archives – to evidence – supports democracy, transparency and accountability and helps foster a sense of personal and collective identity. My government, therefore, protects and makes available documentary evidence, information, records and archives in order to support accountability, identity and memory.

In its deliberations, the Committee affirmed Laura Millar's vision for an information management regime within government. It also saw government as moving in the right direction with its intended implementation of the new *Information Management Act*.

The Committee agreed there is a need for a cohesive and robust set of requirements that apply to the whole of government throughout the entire life-cycle of records – from a duty to document through to archiving. The Committee emphasized the importance of archiving, in particular, because it provides convenient access to historical records for researchers and institutional memory for decision-makers. Archiving is a key enabler of good and accountable government in a democratic society, and should be seen as a priority within government's information management scheme.

Recommendations

The Committee recommends to the Legislative Assembly that the provincial government:

3. Make all obligations related to the entire life-cycle of government records part of a cohesive and robust information management scheme; and

4. Ensure that archiving is a high priority.

Data Sovereignty (s. 30.1)

Section 30.1 of FIPPA requires public bodies to ensure that personal information in their custody or control is stored and accessed only in Canada unless certain exceptions apply. Those exceptions are (a) where the individual the information is about has consented to it being stored in or accessed from another jurisdiction, (b) if the personal information is stored in or accessed from another jurisdiction for the purpose of a disclosure authorized under FIPPA, or (c) if the personal information was disclosed for the purposes of a payment made to or by government or a public body.

This data sovereignty, or data residency, requirement ensures that all personal information is protected in accordance with Canadian law, and therefore not at risk of being subject to a lesser degree of privacy protection because of lower standards that may exist in other jurisdictions. One consequence of this requirement, among other things, is that it may prevent public bodies from using cloud-based solutions and other information technologies that are only available outside Canada. During its public consultation process, the Committee heard opposing views as to whether s. 30.1 should be amended to permit storage or access outside Canada under certain conditions.

A number of public bodies, including health authorities, post-secondary institutions, school districts, TransLink, the Insurance Corporation of British Columbia ("ICBC"), BCNET, and the College of Registered Nurses of BC all voiced concerns about how the existing data sovereignty requirement affected their business activities, and day to day operations.

In a joint submission, Vancouver Coastal Health Authority, Vancouver Island Health Authority, Fraser Health Authority, Northern Health Authority, and Providence Healthcare Society described challenges it presents for them, including impairing their ability to use technologies, global expertise, and data services; and negative impacts such as costs, staff and patient frustration, reduced functionality in IT systems, and having to respond to breaches.

Similarly, the Research Universities' Council of BC, speaking on behalf of the University of British Columbia, Simon Fraser University, University of Victoria, University of Northern British Columbia, Royal Roads University, and Thompson Rivers University, identified negative impacts on administrative efficiency and security, international engagement and student recruitment, online learning offerings, and academic integrity.

In essence, both health authorities and the Research Universities' Council thought s. 30.1 lacks proportionality. In their view, public bodies should be permitted to store and disclose personal information outside Canada for limited purposes and under certain conditions that would mitigate risks to privacy. The health authorities recommended amending s. 30.1 to authorize

public bodies to store and disclose personal information outside Canada when (a) it relates directly to and is necessary for a program or activity of the public body; (b) security measures proportional to the risk posed by the type(s), sensitivity, volume and location of personal information are in place; and (c) the Commissioner is provided with the privacy impact assessment for information. The Research Universities' Council recommended slightly different conditions: (a) it relates directly and is necessary for a public program or activity; (b) there is no reasonable alternative in Canada; (c) security measures are in place depending on the type of information; (d) it is impractical to obtain consent; and (e) the privacy impact assessment is shared with the Commissioner for review and comment.

The Canadian Bar Association agreed that s. 30.1 should be amended to give public bodies the discretion to store or access personal information outside Canada under limited circumstances where the benefit of doing so clearly outweighs the potential harm. The Association's position is that this would allow public bodies to perform their mandates more effectively, in the spirit of the Act, and would ensure compliance with international standards and treaty obligations.

Public advocacy organizations were not in favour of amending s. 30.1. The Canadian Centre for Policy Alternatives, the BC Civil Liberties Association, and the BC Freedom of Information and Privacy Association believe that the prohibition against storage and access outside Canada should be retained. As stated by the BC Civil Liberties Association, it provides necessary and critically important protection for the personal information of British Columbians.

In response to a query from a Committee Member at her appearance before the Committee on November 18, 2015, the Information and Privacy Commissioner indicated that she wished to see the prohibition remain as is. She said:

> The Maple Leaf constitutional protection does not follow our data when it leaves the country, whether it goes to the US and it's in the hands of the cloud provider or elsewhere. Essentially, the concerns that led the Legislature to make the data localization provision 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.

In her written response to recommendations made to the Committee during its public consultation process, the Information and Privacy Commissioner responded to concerns that were raised by public bodies regarding the impacts of s. 30.1 on their operations. She stated that:

> Several submissions noted the limited options available to public bodies for cloud services hosted within Canada, but recently we have seen the market respond to the

demand for storage in Canada. Last year Microsoft and Adobe announced they will be offering cloud-based storage and software applications within Canada and this year Amazon, the largest cloud services provider in the world, made a similar announcement. Developments like these will make it increasingly easier and more affordable for public bodies to access cloud solutions in compliance with FIPPA.

In its submission, government acknowledged the challenges that public bodies face because of the data sovereignty requirement, but maintained that retention of the provision is likely the right approach. It cited a recent decision of the European Court of Justice to invalidate the US-EU Safe Harbor Framework as an example that strengthens the case for data sovereignty in BC. Government wishes to continue to monitor changes to privacy laws in other jurisdictions, especially the European Union General Data Protection Regulations, to ensure that its approach remains harmonized and that it also monitors emerging technology solutions to ensure that the data residency requirements remain relevant and practical in a changing technical environment.

The Committee is in agreement with privacy advocates that the personal information of British Columbians should be protected in accordance with Canadian law. Should it be stored or access outside Canada, there is a risk that it could be subject to a lower standard of privacy protection. Committee Members discussed the use of encryption, tokenization, and other technological solutions to de-identify data so that it is no longer personal information, and noted that the Information and Privacy Commissioner has provided guidance to public bodies on how to deploy tokenization in such a way that it complies with the restriction in s. 30.1. The Committee also noted that s. 30.1 is not an absolute prohibition, and that public bodies may store or allow access outside Canada with the consent of the individual the information is about, if the disclosure is permitted under FIPPA, and for the purposes of a payment made to or by government or a public body.

While the Committee appreciates the concerns expressed by health authorities, universities, schools, and other public bodies regarding their inability to use new innovative technology in their operations, the Committee is not persuaded that there are no available or adequate alternatives that do not involve storage or access outside Canada. The Committee agrees with government that it should continue to monitor changes in privacy laws and in technology solutions to ensure that the provision remains harmonized and that it is relevant and practical.

Recommendation

The Committee recommends to the Legislative Assembly that the provincial government:

5. Retain the data sovereignty requirement in s. 30.1 of FIPPA.

The Application of FIPPA to Subsidiary Corporations and Other Entities

The Committee received 18 submissions from individuals and organizations advocating that FIPPA apply to subsidiary corporations and other entities that are publicly funded. In some cases, they referenced particular subsidiary corporations or entities that should be subject to FIPPA. The AMS Student Society of UBC Vancouver focused on the "corporate veil" problem at universities and school boards where it appears the public body established a wholly-owned and controlled subsidiary for the purpose of withholding records. The Ubyssey and Devin Todd specifically named wholly-owned subsidiaries of the University of British Columbia (UBC Properties Trust and/or UBC Investment Management Trust). Adam Waitzer also said that the public deserves access to documents of a privately held subsidiary of the University of British Columbia. Rob Wipond specifically named the BC Association of Chiefs of Police and the BC Association of Municipal Chiefs of Police. Owen Munro and James Smith from Langara College were of the view that student governments and student unions should be covered under FIPPA.

Other submissions set out criteria for the application of FIPPA to subsidiary entities. CUPE BC Division and the Canadian Centre for Policy Alternatives stated that:

> FIPPA should cover any board, committee, commission, panel, agency or corporation that is created, controlled or owned by a public body or group of public bodies.

The Canadian Bar Association suggested that any amendments intended to capture subsidiary agencies of public bodies should apply only to legal entities rather than boards, committee, or panels and it should not apply to corporations owned exclusively for investment purposes.

Several submissions recommended a wider application of FIPPA beyond only subsidiary entities. The Centre for Law and Democracy stated that FIPPA should apply to any organization which either receives public funding or performs a public function to the extent of that funding or function. The BC Government and Service Employees' Union expressed this concept as the need to clarify the definition of "public bodies" in order to make sure no public or government-related services, bodies, associations, or subsidiaries are beyond the reach of the legislation and its provisions.

In his presentation to the Committee on November 9, 2015, Stanley Tromp recommended amending FIPPA to state that its coverage extends to:

> any institution that is established by the Legislature or by any public agency that is publicly funded or publicly controlled, or 50 percent or more owned, or performs a

public function is vested with public powers or has a majority of its board appointed by it.

The Information and Privacy Commissioner recommended a specific change to the wording of the definition of "public body" in FIPPA in order to extend its coverage to subsidiary entities, including corporations, panels, or agencies. This is to replicate paragraph (n) of the definition of "local government body" and add it to the definition of "public body" in Schedule 1. Paragraph (n) reads as follows:

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

The definition of public body in FIPPA would then read as follows:

> "public body" means
>
> (a) a ministry of the government of British Columbia,
>
> (b) an agency, board, commission, corporation, office or other body designated in, or added by regulation to, Schedule 2,
>
> (c) a local public body, or
>
> (d) any board, committee, commissioner, panel, agency or corporation that is created or owned by a body referred to in paragraphs (a) to (c) and all the members or officers of which are appointed or chosen by or under the authority of that body,
>
> but does not include
>
> (e) the office of a person who is a member or officer of the Legislative Assembly, or
>
> (f) the Court of Appeal, Supreme Court or Provincial Court.

The Commissioner's position with respect to subsidiary entities was echoed by CUPE Local 116 in its presentation to the Committee on November 9, 2015.

In her response to submissions to the Committee, the Commissioner went further and indicated that she supported the recommendation of the Centre for Law and Democracy that FIPPA be extended to cover any entity that is performing a public function:

> Apart from the subsidiary issue, there will be other cases where a question arises as to whether an entity should be considered a public body within the meaning of the Act. An entity could be created by more than one public body, or it may be a mix of public and private bodies. An entity could have members or officers that are appointed by more than one public body or represent a mix of public and private body appointments. It could also be an entity that is clearly carrying out a public function but that does not meet the definition of public body.

She suggested that this broader application could be achieved by amending s. 76.1 of FIPPA to authorize the minister to add to Schedule 2 a body that is performing a public function.

Government spoke to the application of FIPPA during its presentation to the Committee on November 18, 2015. Government advised the Committee that it intends to make the BC Association of Chiefs of Police subject to FIPPA. Government is drafting an amendment that will change the definition of a "local public body" to include a police association. This change would include the BC Association of Chiefs of Police and would allow the BC Association of Municipal Chiefs of Police to be covered if it were to become a legal entity. In response to a question from a Committee Member, government advised the Committee that government intends to extend the application of FIPPA to subsidiary corporations but that it is a complex task, and government is in the process of consulting with public bodies on developing a set of criteria on how that should be accomplished.

The previous statutory review committee recommended in its 2010 report that government 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 Committee endorsed that recommendation. It agreed that subsidiaries and other entities created or owned by public bodies should be subject to FIPPA and accepted the Commissioner's specific recommendation on how the definition of "public body" in Schedule 1 should be amended to accomplish that. The Committee did not, however, support a broader scope of application.

During their deliberations, Members also discussed whether certain specific entities should be designated as public bodies. They were in favour of government's proposed amendment that would include the BC Association of Chiefs of Police and the BC Association of Municipal Chiefs of Police as local public bodies. They noted that Providence Health Care and the First Nations Health Authority are not public bodies under FIPPA. The Committee also noted that Tsawwassen Institutions are subject to the 2009 Tsawwassen First Nation *Freedom of Information and Protection of Privacy Act*.

Recommendations

The Committee recommends to the Legislative Assembly that the provincial government:

6. Extend the application of FIPPA to any board, committee, commissioner, panel, agency or corporation that is created or owned by a public body and all the members or officers of which are appointed or chosen by or under the authority of that public body; and

7. Consider designating all publicly-funded health care organizations as public bodies under FIPPA.

The FOI Process

The access to information provisions in FIPPA give individuals the right to make an access request and mandate how public bodies respond. This is commonly known as the FOI process. The principle behind the FOI process is that information should be released unless there is a good reason not to release.

FIPPA sets out an administrative process that public bodies must follow in responding to an access request. That process includes time limits and extensions, a duty to assist, fees and fee waivers, and a complaints mechanism. Public bodies are also permitted, or in some cases required, to refuse to release certain types of information.

Some public bodies post on their websites all or some of their responses to access requests that do not contain personal information. For example, as previously discussed, government has "information releases" available on the open information page of its website. Through this mechanism, responses to access requests are made available to the public.

Time limit for responding to access requests (s. 7)

Section 7 of FIPPA requires public bodies to respond to an access request within 30 business days of receiving it. A 30 day time limit is relatively standard across Canada but "day" is defined in Schedule 1 to not include a holiday or a Saturday, resulting in a longer time limit than in most Canadian jurisdictions. The Committee heard different opinions about a timeline of 30 business days.

Several participants in the Committee's public consultation process, including the Canadian Centre for Policy Alternatives, Stanley Tromp, the Centre for Law and Democracy, CUPE BC Division, and Stephen Bohus, thought this time limit should be reduced from 30 to 20 or even 14 calendar days to ensure public bodies are responding to requests in a timely manner. CUPE BC Division pointed out that requests are very often time sensitive, dealing with current issues or those in the very recent past. It stated:

> CUPE's use of FOI requests almost always involves the need to obtain information involving matters of current or imminent public concern – this is true whether they pertain to considerations of broad community concern or very specific labour related issues. It is evident that the same would be true for community groups, academics and certainly the media.

Public bodies had other views. The Regional District of Kootenay thought the time limit should remain as 30 business days. TransLink asked that public bodies be permitted to postpone

responding to access requests when the same individual has submitted more than five access requests. The City of Surrey raised the issue of abandoned requests and suggested that a public body should be able to declare a request abandoned if the applicant fails to respond within 30 days.

In its deliberations, the Committee agreed that the FOI process should be as efficient as possible, and that individuals deserve timely responses to their access requests. It therefore concluded that the time public bodies have to respond to access requests should be reduced from 30 business days to 30 calendar days.

Time extensions (s. 10)

Section 10 of FIPPA allows a public body to extend the time for responding to an access request for up to 30 days if certain conditions are met, such as when the applicant consents to the extension. The public body may further extend that deadline with the permission of the Information and Privacy Commissioner.

The Committee received seven different submissions regarding time extensions. Most expressed concerns about delays and recommended that either the length of time should be reduced or that all extensions require the approval of the Information and Privacy Commissioner. The Canadian Centre for Policy Alternatives thought that public bodies should be required to keep applicants informed of decisions in relation to extensions. The BC Lottery Corporation was of the view that public bodies should be allowed to take an extra time extension in the event of unusual or catastrophic circumstances.

Time permitted for transferring a request (s. 11)

Section 11 of FIPPA permits a public body to transfer an access request to another public body within 20 days of receiving the request if the record is under the custody or control of the other public body. Two public interest advocacy organizations suggested changes to the 20-day transfer period. The Centre for Law and Democracy said that the 20-day period is longer than necessary. The BC Freedom of Information and Privacy Association thought that the 20-day transfer period should be eliminated because government has a centralized system for handling access requests.

In 2010, the previous statutory review committee recommended that s. 11 be amended to reduce the time allowed for file transfers to ten business days. The Committee was not prepared to make a recommendation as to the exact number of days that would be appropriate but urges government to review the timelines for extensions and transfers with a view to reducing them in order to ensure an efficient, timely, and responsive FOI process.

Recommendations

The Committee recommends to the Legislative Assembly that the provincial government:

8. Reduce the timeline in which a public body must respond to an access request from 30 business days to 30 calendar days.

9. Review other timelines established in FIPPA with a view to reducing them in order to ensure the efficiency and timeliness of the FOI process.

Protect anonymity of applicants

The Information and Privacy Commissioner recommended that public bodies be required to ensure that the name and type of applicant is only disclosed to the employee of the public body who receives the access request, subject to limited exceptions. She argued that in the absence of such a requirement, it opens the applicant to possible discrimination and appears to negatively influence response times. The BC Civil Liberties Association agreed that there should be a legislative requirement for the anonymity of requesters, as did Stanley Tromp.

In response to questions from Members as to how public bodies would be able to continue to collect statistical information about applicants, the Commissioner advised that this could be done by having the first point of contact for the public body specifically tasked with processing access requests to be responsible for those statistics without the involvement of the program area that is responsible for processing access requests.

The Information and Privacy Commissioner identified s. 12 of the Newfoundland and Labrador *Access to Information and Protection of Privacy Act* as a good precedent for such a provision. It reads as follows:

12. (1) The head of a public body shall ensure that the name and type of the applicant is disclosed only to the individual who receives the request on behalf of the public body, the coordinator, the coordinator's assistant and, where necessary, the commissioner.

(2) Subsection (1) does not apply to a request

(a) respecting personal information about the applicant; or

(b) where the name of the applicant is necessary to respond to the request and the applicant has consented to its disclosure.

(3) The disclosure of an applicant's name in a request referred to in subsection (2) shall be limited to the extent necessary to respond to the request.

(4) The limitation on disclosure under subsection (1) applies until the final response to the request is sent to the applicant.

Previous statutory review committees in 2004 and 2010, recommended such a provision:

> Amend section 4(1) to establish that an applicant who makes a formal access request has the right to anonymity throughout the entire process.

Government advised the Committee that its response to the 2010 recommendation was to address this issue through policy and training because this would accomplish the goal more directly and completely.

In its March 16, 2016 written submission, government elaborated on its position:

> Current privacy provisions in FOIPPA already protect the identities of individuals who make FOI requests, ensuring that the names of applicants are only shared on a "need to know" basis. Further protection would add little value and could limit public bodies' ability to provide the best service to applicants.
>
> To ensure that knowledgeable employees are able to assist applicants with their requests, specific criteria for the protection and provision of an applicant's identity for the purpose of processing an FOI request should continue to be governed by policy.

The Committee does not agree with government's position. The right to anonymity during the FOI process should be entrenched in legislation, as it is in the Newfoundland and Labrador statute, in order to properly protect the name and type of applicant.

Recommendation

The Committee recommends to the Legislative Assembly that the provincial government:

10. Amend s. 4(1) of FIPPA to establish that an applicant who makes a formal access request has the right to anonymity.

Mandatory Breach Notification and Reporting

Mandatory breach notification and reporting would require public bodies to notify affected individuals about an unauthorized disclosure of personal information (a "privacy breach") where there is a risk of significant harm. Public bodies would also be required to report the privacy breach to the Office of the Information and Privacy Commissioner so that the office can assist public bodies to manage the breach, address its root cause, and help to prevent future occurrences.

As defined in the 2015 federal *Digital Privacy Act*, and the 2015 Newfoundland and Labrador statute, "significant harm" may include bodily harm, humiliation, damage to reputation or relationships, loss of employment or business opportunities, financial loss, identity theft, negative effects on the credit record, and damage to or loss of property.

The Information and Privacy Commissioner submitted that FIPPA should mandate breach notification and reporting for the following reason:

> FIPPA requires public bodies to be responsible for protecting personal information against such risks as loss or unauthorized access, collection, use, disclosure, or disposal. Every public body should have breach protocols in place to uphold this responsibility. Breach notification and reporting should be an explicit requirement under FIPPA when a privacy breach occurs, because it supports individuals in taking measures to mitigate the harm that can arise from a breach, provides clarity about when to notify and report, and reduces the incidents of breaches going forward.

The Information and Privacy Commissioner recommended that the reporting framework include:

- 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 the 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.

The new Newfoundland and Labrador *Access to Information and Privacy Act, 2015* and recent amendments to the federal *Personal Information Protection and Electronic Documents Act* (not in force) include mandatory breach notification and reporting. The Alberta *Personal Information Protection Act*, the Nunavut *Access to Information and Protection of Privacy Act*, and several health information privacy laws in other provinces also mandate breach notification and reporting.

In addition to the Information and Privacy Commissioner, four advocacy organizations, namely the BC Freedom of Information and Privacy Association, the BC Civil Liberties Association, the Canadian Bar Association, and the National Association for Information Destruction – Canada, proposed that mandatory breach notification and reporting be added to FIPPA. The BC Civil Liberties Association said that notification is the only effective means by which individuals can take steps to mitigate the harms of a breach; and reporting is needed to bring the expertise of the Office of the Information and Privacy Commissioner to bear on reducing incidents of future breaches. The Canadian Bar Association recommended adding to FIPPA a provision similar to s. 37.1 of the Alberta *Personal Information Protection Act*, and that the form and content of notices in the event of breaches should be in regulations.

One public body spoke of internal reporting mechanisms. The City of Surrey stated that it should be a requirement to notify the head of the public body and the head of the IT department of a potential privacy breach, and that the obligation to notify affected individuals should be the responsibility of the head.

In its written submission to the Committee, government indicated that comprehensive consultation should be conducted with impacted public bodies on the scope, wording and timing of any proposed amendment to FIPPA that requires the mandatory notification and reporting of privacy breaches.

In the view of the Committee, mandatory breach notification and reporting by public bodies is in the public interest. It reflects best practices that are entrenched in other privacy laws in Canada, and are being increasingly recognized internationally. Its inclusion in the statutory framework of FIPPA would help to mitigate the risks to British Columbians in the event of a privacy breach, and prevent future ones from occurring. The Committee accepts the proposed framework for mandatory breach notification as recommended by the Information and

Privacy Commissioner with the additional authority for the Information and Privacy Commissioner to order notification to the public when it is appropriate to do so.

Recommendation

The Committee recommends to the Legislative Assembly that the provincial government:

11. Add a mandatory breach notification and reporting framework to FIPPA that 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 the 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 or the public; and
    - a requirement that public bodies document privacy breaches and decisions about notification and reporting.

Other Recommendations

Access

Duty to Assist (s. 6)

Section 6 of FIPPA requires public bodies to make every reasonable effort to assist applicants. Sara Levine, Q.C., suggested that s. 6 be amended to require public bodies to make available basic contact information about the person responsible for receiving requests for access to information and other inquiries about access and privacy rights. She noted that there is such a requirement in BC's private sector privacy law. Pursuant to s. 4(5) of the *Personal Information Protection Act*, organizations must make the contact information of the person responsible for ensuring compliance available to the public.

The Committee discussed concerns regarding compliance within government and other public bodies with the duty to assist under FIPPA and concluded that adding this specific concrete measure as a statutory requirement would enhance the FOI process.

Recommendation

The Committee recommends to the Legislative Assembly that the provincial government:

12. Amend s. 6 of FIPPA to add a specific requirement for public bodies to make the contact information of the person responsible for ensuring compliance available to the public.

Exceptions to Access to Information

Access laws generally either require or permit public bodies to refuse to disclose certain types of information. These are known as mandatory and discretionary exceptions and reflect a balancing of access to information with the protection of other interests that would be adversely affected by disclosure of such information.

Mandatory exceptions in FIPPA include cabinet confidences, tendering or other information that may cause harm to the business interests of a third party, and personal information if the

disclosure would be an unreasonable invasion of a third party's personal privacy. Discretionary exceptions include policy advice and recommendations, legal advice subject to solicitor-client privilege, and information the disclosure of which would be harmful to law enforcement, intergovernmental relations, or the financial or economic interests of a public body.

Many participants in the Committee's public consultation process spoke to the need for changes to focus and narrow exceptions to disclosure and better serve the goal of freedom of information and accountability. Other participants thought that the exceptions should either be retained as is, or broadened to permit public bodies to withhold certain types of information in order to serve other important public policy purposes. The Committee also heard proposals to change a mandatory exception to a discretionary exception and vice versa. The diverse recommendations the Committee received with respect to exceptions to access to information are set out below together with the Committee's conclusions and recommendations.

Mandatory Exceptions

Cabinet Confidences (s. 12)

Section 12 of FIPPA prohibits the disclosure of information that would reveal the substance of deliberations of cabinet or any of its committees. This prohibition does not apply to records that have been in existence for 15 or more years.

The BC Freedom of Information and Privacy Association, the Canadian Centre for Policy Alternatives, CUPE BC Division, and Stanley Tromp submitted that the provision should be discretionary rather than mandatory. The BC Freedom of Information and Privacy Association and the Centre for Law and Democracy also submitted that the exception be shortened to records that have been in existence for ten years.

The Information and Privacy Commissioner indicated that she supports the recommendation to make the exception of cabinet confidences discretionary rather than mandatory provided that only cabinet, and not the head of a public body, is able to exercise this discretion. She noted the precedent for cabinet exercising this discretion under s. 16 in relation to information which could reasonably be expected to harm inter-governmental relations or disclose inter-governmental confidences.

In 2010, the previous statutory review committee considered whether to amend the mandatory exception in s. 12, and concluded that it was undesirable to make confidential records more accessible at this time.

Committee Members discussed whether the exception for cabinet confidences should be a discretionary exception in order to permit cabinet to disclose cabinet confidences in a case where cabinet believes that the public interest in the disclosure of the information outweighs the need to protect the cabinet confidence. For example, cabinet may wish to disclose records in order to address a public controversy regarding one of its decisions.

Committee Members noted that, while the protection of cabinet confidences is generally a mandatory exception in Canadian jurisdictions, the 2015 Newfoundland and Labrador access to information statute permits the Clerk of the province's Executive Council to disclose a record or information that would reveal the substance of deliberations of cabinet where the Clerk is satisfied that the public interest in the disclosure of the information outweighs the reason for the exception. The Committee concluded that s. 12 should be amended along these lines to permit cabinet to disclose records if it is in the public interest to do so. This amendment would allow government to recognize the overall public interest as a basis for waiving the protection of confidentiality of cabinet decisions.

Recommendation

The Committee recommends to the Legislative Assembly that the provincial government:

13. Amend s. 12 of FIPPA to permit the Cabinet Secretary to disclose to an applicant information that would reveal the substance of deliberations of the Executive Council or any of its committees where the Cabinet Secretary is satisfied that the public interest in the disclosure of the information outweighs the reason for the exception.

Disclosure Harmful to Business Interests of a Third Party (s. 21)

Section 21 of FIPPA prohibits a public body from disclosing information that would significantly harm the competitive position or interfere significantly with the negotiating position of a third party if certain conditions are met.

ICBC and BC Lottery Corporation made submissions with respect to this provision. ICBC proposed that the exception should include information that was provided in the capacity of a customer because the current three part test for financial harm in s. 21 does not adequately

protect commercial customers given not every release of their confidential information meets the financial harm test. ICBC advised that it receives access requests for information about corporate customers' insurance and vehicle registration information and argues that a business should not be exposed to disclosures of its confidential information simply because it is a customer of a public body.

BC Lottery Corporation submitted that third party business interests should be protected where the information is inaccurate or unreliable and its disclosure may unfairly damage the reputation of a business referred to in the requested records.

Committee Members were sympathetic to the concerns of ICBC and BC Lottery Corporation regarding the application of s. 21 in the context of their particular corporate activities. However, they questioned whether the concerns were so serious and widespread that they warranted amendments to FIPPA.

Disclosure Harmful to Personal Privacy (s. 22)

Section 22 of FIPPA prohibits public bodies from disclosing personal information if the disclosure would be an unreasonable invasion of a third party's personal privacy. A public body must consider all of the relevant circumstances in determining whether the disclosure constitutes an unreasonable invasion including whether the information is about a deceased person, and if so, whether the length of time the person has been deceased indicates the disclosure is not an unreasonable invasion of the deceased person's personal privacy.

Lisa Fraser, a parent, submitted that there needs to be a better balance between the rights of the recently deceased and the need for public scrutiny of the decisions of the Ministry of Children and Family Development in order to prevent deaths of youth in care.

The Committee recognized the competing public policy concerns at issue, and concluded that government should consider initiating a review of whether a parent of a child who was in care should have access to personal information about their deceased child.

Recommendation

The Committee recommends to the Legislative Assembly that the provincial government:

14. Consider initiating a review of whether a parent of a child who was in care should have access to personal information about their deceased child.

Disclosure of Information Relating to Abortion Services (s. 22.1)

Section 22.1 of FIPPA prohibits the disclosure of information relating to abortion services except information about abortion services that were received by the applicant; statistical information relating to the total number of abortion services provided in BC or a designated region; and information about a public body's policies on the provision of abortion services.

The Committee received submissions from WeNeedaLAW, United for Life Advocacy Association, the Christian Heritage Party, and individuals advocating the repeal of s. 22.1 of FIPPA. Most argued that the provision unnecessarily limits access to information regarding the expenditure of public funds on a medical procedure. It was also submitted that information related to abortion services is already protected by other exemptions and a letter from former Information and Privacy Commissioner David Loukidelis at the time the provision was added to FIPPA in 2001 was cited in support of that view. In his letter, Mr. Loukidelis objected to the provision as a subject-matter exception that was unnecessary.

The previous statutory review committee stated in its 2010 report that the majority of Committee Members did not support the call to repeal the ban on hospital abortion statistics.

During its deliberations, the Committee recognized the extreme sensitivity of abortion related information. The Committee unanimously decided not to recommend any amendments to s. 22.1.

Discretionary Exceptions

Policy Advice or Recommendations (s. 13)

Section 13 of FIPPA permits a public body to withhold information that would reveal advice or recommendations developed by or for a public body or minister. It does not apply to information in a record that has been in existence for ten or more years.

In 2004, a previous statutory review committee made the following recommendation:

> Amend section 13(1) to clarify the following:
>
> (a) "advice" and "recommendations" are similar terms often used interchangeably that set out suggested actions for acceptance or rejection during a deliberative process,
>
> (b) the "advice" or "recommendations" exception is not available for the facts upon which advised or recommended action is based; or for factual, investigative or background material; or for the assessment or analysis of such material; or for professional or technical opinions.

In 2010, the majority of members of the previous statutory review committee concluded that it was prudent to maintain the advice exception for evidence-based interpretations, analyses and recommendations and did not endorse the 2004 recommendations.

In their submissions to the Committee, the Information and Privacy Commissioner, the Canadian Centre for Policy Alternatives, the BC Civil Liberties Association, and CUPE BC Division indicated they endorse the 2004 recommendation as a necessary clarification that the exception does not extend to the facts upon which the advice or recommendation is based.

In her written submission, the Information and Privacy Commissioner advised that since the 2010 recommendation was made, "advice" and "recommendations" have been interpreted by the courts as having different meanings. This has broadened the application of s. 13 to any document compiled in the course of considering alternative options, including factual material and expert opinions. The Information and Privacy Commissioner argued this is contrary to the original intent of this provision, and essentially reiterated the 2004 recommendation as follows:

> 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 background materials, for the assessment or analysis of such material, or for professional or technical opinions.

The BC Freedom of Information and Privacy Association proposed narrowing the provision to include only information which recommends a decision or course of action by a public body, minister, or government. Stanley Tromp advocated adding a harms tests (i.e. the record could only be withheld if disclosing it would cause serious or significant harm to the deliberative process) and that the exception would not apply after a final decision on the matter is completed and made public.

The Canadian Centre for Policy Alternatives also suggested reducing the time limit for withholding the records from ten to five years.

Committee Members affirmed that the exception of s. 13(1) is necessary because of the need for officials to be able to give advice and make recommendations to senior executive and ministers freely and frankly. In considering whether that exception should apply to the facts upon which the advice or recommendations are based, the Committee took note of the intention of the Legislative Assembly as evidenced by s. 13(2)(a), which requires public bodies to disclose factual material and the Information and Privacy Commissioner's submission that s. 13(1) should be clarified to address court rulings. The Committee concluded that the facts upon which the advice or recommendations are based should not come within the exception of s. 13(1) (although this may be covered by other exception such as cabinet confidences). The Committee recommends that s. 13(1) be amended to the extent that is necessary to provide clarification as recommended by a previous statutory committee in 2004.

Recommendation

The Committee recommends to the Legislative Assembly that the provincial government:

15. Amend s. 13(1) of FIPPA to clarify that the discretionary exception for "advice" or "recommendations" does not extend to facts upon which they are based; or for factual, investigative or background material; or for the assessment or analysis of such material; or for professional or technical opinions.

Legal Advice [Solicitor-Client Privilege] (s. 14)

Section 14 of FIPPA permits a public body to refuse to disclose information in response to an access request that is subject to solicitor-client privilege. The Committee heard a range of views on whether the provision should be amended.

Ryan Berger suggested that the exception be broadened to ensure that all types of legal privilege are protected (litigation privilege and settlement privilege). The Centre for Law and Democracy, on the other hand, stated it should be limited to litigation privilege. Robert Botterell maintained that the provision does not need to be amended.

The Law Society of BC told the Committee that the provision should be made mandatory 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. The Law Society stated that its concern is that, by giving the head of a public body the discretion to refuse to disclose information that is subject to solicitor-client privilege, it appears by implication to give discretion to disclose privileged information. It submitted that "The confidential relationship takes precedence over the rights of third parties to information, and only the client has the option of releasing privileged information arising from that relationship."

The Law Society also suggested amending s. 44(3) to exclude from disclosure to the Commissioner all records that are subject to solicitor-client privilege.

J.C. Hunter suggested a deeming provision such that where a public body official acted contrary to legislation, and where the official revealed a portion or gist of a legal opinion publicly to defend himself, the official should be deemed to have waived privilege over the entire legal opinion.

The Information and Privacy Commissioner indicated that she does not support the Law Society's recommendation because she is not aware of any instance where a public body has disclosed information that was subject to solicitor-client privilege but where the client was not the public body or did not consent to the disclosure. She also questions whether there is, in fact, a problem that needs to be fixed.

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

In 2010, the previous statutory review committee supported the position of the Law Society and made the following recommendation:

> 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.
>
> 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.

The Committee endorsed the 2010 recommendation to make s. 14 a mandatory exception for reasons of clarity, certainty, and consistency with case law. There appears to be no basis for solicitor-client privilege to be a discretionary exception. The public body has a duty to protect privileged information in all cases unless privilege is waived by the client.

With respect to the recommendation that decisions as to whether or not records are privileged should be made by the Supreme Court rather than the Office of the Information and Privacy Commissioner, the Committee is satisfied with the status quo and believes it is appropriate that those decisions be made by the Office of the Information and Privacy Commissioner.

Recommendation

The Committee recommends to the Legislative Assembly that the provincial government:

16. Amend s. 14 of FIPPA to make it a mandatory exception unless 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.

Disclosure Harmful to Law Enforcement (s. 15)

Section 15 of FIPPA permits a public body to refuse to disclose information if the disclosure could reasonably be expected to harm a law enforcement matter. The Committee heard two different perspectives on how this provision should be amended.

The BC Freedom of Information and Privacy Association suggested narrowing the exception by adding the word "active" before law enforcement. From its perspective as a professional regulatory body, the Law Society of BC proposed that the definition of "law enforcement" in Schedule 1 be expanded because investigations about credentials, investigations leading to voluntary remediation, and audits of trust accounts that do not lead to disciplinary proceedings involving a penalty or sanction may not fall within the definition of "law enforcement."

The Law Society recommended that "law enforcement" be defined to include proceedings or investigations conducted by a professional governing body in furtherance of its duties and obligations in the public interest. Alternatively, the Law Society recommended using more specific and restrictive language to define "law enforcement" as it applies to professional governing bodies:

> Proceedings or investigations conducted by a professional governing body in furtherance of its duties and obligations in the public interest, including but not limited to investigations or audits regarding:
>
> i. the qualifications, character and fitness of an individual to become a member of the professional governing body or to be enrolled as a student under the authority of the professional governing body,

ii. the ability of a member of a professional governing body to practise and continue to practise a profession,

iii. a complaint or allegation or other information concerning the conduct of a member or former member of a professional governing body or a student under the authority of the professional governing body, and

iv. compliance with rules or regulations governing the professions.

The Information and Privacy Commissioner was of the view that the Law Society's proposed expansion of the definition of law enforcement is unnecessary because the definition includes investigations or proceedings that lead, or could lead, to a penalty or sanction being imposed and confidentiality concerns are addressed in s. 22 of FIPPA where disclosure may be harmful to personal privacy.

Committee Members concluded that it was not entirely clear whether s. 15 and the existing definition of "law enforcement" or s. 22 adequately address the concerns of the Law Society that it could not refuse to disclose certain information during the conduct of an investigation that could conceivably harm that investigation. The Committee recommended that government consider whether an explicit reference to an investigation of a professional regulatory body should be added to the definition of "law enforcement" for greater certainty.

Recommendation

The Committee recommends to the Legislative Assembly that the provincial government:

17. Consider whether an explicit reference to investigations that are within the mandate of a professional regulatory body should be added to the definition of "law enforcement" in Schedule 1 so that a professional regulatory body may refuse to disclose information that may harm an investigation.

Disclosure Harmful to Intergovernmental Relations or Negotiations (s. 16)

Section 16 of FIPPA permits a public body to refuse to disclose information that could harm the conduct of intergovernmental relations or negotiations. The Centre for Law and Democracy submitted that this exception is unnecessary because it is already covered by the exception from disclosure of information harmful to commercial or financial interests and information about negotiations (s. 17).

The Committee noted that the protection of intergovernmental relations or negotiations is widely recognized as being important for the broad economic and political interests of the province, and concluded that sufficient evidence had not been presented to demonstrate clearly that the exception for information harmful to intergovernmental relations is redundant.

Disclosure Harmful to the Financial or Economic Interests of a Public Body (s. 17)

Section 17 of FIPPA permits a public body to refuse to disclose information if the disclosure could reasonably be expected to harm the financial or economic interests of a public body or government or the ability of government to manage the economy. Under s. 17(1)(d), this includes information the disclosure of which could reasonably be expected to result in the premature disclosure of a proposal or project or in undue financial loss or gain to a third party.

The BC Lottery Corporation recommended amending s. 17(1)(d) to replace the word "undue" with the word "any" in order to lessen the burden of proof and better protect commercially sensitive information of public bodies, and commercial Crown corporations in particular, as primarily revenue-generating public bodies.

The Information and Privacy Commissioner advised that she does not support a special accommodation for Crown corporations, or a lowering of the threshold for applying s. 17. She stated:

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

The Committee accepts the Commissioner's position that the test of reasonableness addresses BC Lottery Corporation's concern, and that it is not necessary to lower the threshold from undue financial loss or gain to any financial loss or gain.

Information That Will Be Published or Released Within 60 days (s. 20)

Section 20 of FIPPA permits a public body to refuse to disclose information that is to be published or released to the public within 60 days of receiving the access request.

ICBC advocated expanding this section to permit public bodies to refuse to disclose documents which have not already been provided and are not otherwise available to the applicant. This would permit ICBC to refuse to disclose records which could be obtained by other means such as through the production of documents during litigation.

The Information and Privacy Commissioner indicated that she does not support this recommendation because the amendment is unnecessary and would limit the right of access. She advised that orders made by her office have said that the availability of records through the Rules of Court or some other process does not displace or prevent the exercise of access rights under FIPPA.

The Committee concluded that public bodies should not have the ability to refuse access requests because there may be other ways for applicants to obtain information. The FOI process should not be a process of last resort, and the fundamental and important information rights under FIPPA should not be undermined by, or considered as being secondary to, other means to obtain information. Such an amendment could undermine access rights in British Columbia, and is therefore not in the public interest.

Redefine Contact Information of Employees of Public Bodies

Schedule 1 of FIPPA defines contact information as, "information to enable an individual at a place of business to be contacted and includes the name, position name or title, business telephone number, business address, business email or business fax number of the individual." Contact information is not personal information. The definition of "personal information" in Schedule 1 is "recorded information about an identifiable individual other than contact information."

ICBC expressed a concern that its employees are frequently contacted for non-work related purposes. It submitted that contact information should be redefined as business contact information along the lines of the definition in the federal *Personal Information Protection and Electronic Documents Act*. That definition reads as follows: "any information that is used for the purpose of communicating or facilitating communication with an individual in relation to their employment, business or profession such as the individual's name, position name or title, work address, work telephone number, work fax number or work electronic address."

The Information and Privacy Commissioner advised that she does not support this proposed amendment because it is unnecessary. The issue raised by ICBC has been addressed in orders of her office stating that information sought for reasons other than a business purpose is not "contact information."

Based on the response of the Information and Privacy Commissioner to this proposed amendment, the Committee concluded that no amendment is necessary.

Fees

Section 4(3) of FIPPA provides that the right of access to a record is subject to the payment of any fee required under s. 75. Section 75 specifies that applicants must pay for certain services, including locating, retrieving and producing the record; preparing the record for disclosure; shipping and handling the record; and providing a copy of the record. Pursuant to s. 75(5), a public body may waive fees at the request of an applicant, if the applicant cannot afford the payment or for any other reason it is fair to excuse payment, or the record relates to a matter of public interest, including the environment or public health or safety. An applicant may make a complaint to the Information and Privacy Commissioner that a fee is inappropriate and the Commissioner may investigate and attempt to resolve the complaint. Schedule 1 of the FIPPA Regulation sets out the amounts of fees.

The Committee received 12 different submissions from individuals, organizations, public bodies, and public interest advocacy organizations that touched on the matter of fees.

Amounts of Fees

In terms of the amounts of fees, Rob Botterell suggested an affordable flat fee that includes up to 200 pages of photocopying. The Canadian Centre for Policy Alternatives proposed increasing the hours of free search time. The Centre for Law and Democracy said that charging for employee time in responding to an access request is not in line with international standards. It recommended amending the fee schedule to reflect the actual costs incurred by public bodies in reproducing or delivering information. Stephen Bohus commented that there should be reasonable fees or no fees at all and that seniors and low-income people should be exempt.

The Committee also heard from public bodies on the matter of fees. The Law Society suggested that public bodies be permitted to charge for all services that are useful or reasonable in the processing of a request made by a commercial applicant. TransLink proposed that the schedule of fees be updated to reflect inflationary increases in the costs of reviewing records, and the current reality that records are increasingly in electronic form.

The Local Government Management Association recommended that the schedule of fees be reviewed to determine whether it is still consistent with the original objectives of the legislation. This recommendation aligns with the 2010 recommendation of the previous statutory review committee that government 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.

During their deliberations, Committee Members affirmed that fees should not be a barrier to access nor are they intended to provide full cost recovery. They should be set at a reasonable level so that the public body can have some assurance that the request is focused and not frivolous, and with the benefit of a modicum of cost recovery, particularly when responses are voluminous and not straightforward. Committee Members discussed the challenges that some public bodies are experiencing in having to respond to multiple access requests from a few individuals. For example, government advised the Committee that a single applicant made over 1,900 access requests to government between April 1, 2011 and March 31, 2016 and the estimated provincial expenditures incurred to provide their requested records during that period totaled approximately $4.3 million. In addition to cost implications, multiple requests may have a negative impact on the ability of public bodies to respond to requests from other individuals in a timely manner. The Committee felt, however, that any limit on the number of legitimate access requests that an individual can make would impair information rights.

The Committee concluded that the schedule of fees should be reviewed with a view to setting them at a level that (a) would not create a barrier to individuals exercising their right to access records, and (b) provides some cost recovery for substantial costs incurred by public bodies in responding to complex requests.

Fee Waivers

As previously discussed, s. 6 of FIPPA requires a public body to make every reasonable effort to assist applicants and to respond without delay to each applicant openly, accurately and completely. Section 7 of FIPPA requires public bodies to respond to an access request within 30 business days.

Several submissions included a recommendation that penalties be added to FIPPA for flagrantly breaching the duty to assist applicants. These included submissions from the BC Freedom of Information and Privacy Association, the BC Civil Liberties Association, CUPE BC Division, the BC Public Interest Advocacy Centre, the Regional District of Central Kootenay, and Larry Lloyd.

The AMS Student Society of UBC Vancouver said that non-compliance could also be addressed through automatic fee waivers. The BC Public Interest Advocacy Centre said that an automatic fee waiver or some other type of penalty would provide a stronger incentive to adhere to FIPPA provisions. It maintained that time limits, extensions, grounds on which a request can be denied, and duty to assist are routinely ignored, and that the current remedy of a complaint or request for review is not sufficient.

The BC Freedom of Information and Privacy Association, the Canadian Centre for Policy Alternatives, and the BC Government and Service Employees' Union also said that there should be an automatic fee waiver for non-compliance with requirements of the FOI process. In addition, BC Government and Service Employees' Union and the Canadian Centre for Policy Alternatives said that fees should be waived if a significant portion of the records have been redacted or blacked out.

The BC Freedom of Information and Privacy Association, the BC Civil Liberties Association, and the BC Public Interest Advocacy Centre suggested that information and assistance be provided to applicants that would facilitate requests for fee waivers. The AMS Student Society of UBC Vancouver and Ubyssey advocated automatic fee waivers for records requested in the public interest.

The Information and Privacy Commissioner was in support of an amendment that would require public bodies to automatically waive fees when a public body fails to meet its legislated timeline for responding to an access request.

The Committee concluded that there should be more opportunities for fees to be waived in order to promote the efficiency of the FOI process and compliance with the timelines established in FIPPA. Committee Members also discussed whether it would add some measure of fairness to the FOI process if there was a fee waiver when all of the records an applicant is seeking are completely severed such that the applicant receives none of the information s/he is seeking. In essence, it amounts to a public body providing no responsive records and Members thought it should be viewed as such and fees reduced accordingly.

Consideration should also be given to making a fee waiver available automatically when responses to access requests disclose records that relate to the public interest. This would mean the applicant would not have to make a specific request for a fee waiver.

Recommendations

The Committee recommends to the Legislative Assembly that the provincial government:

18. Review the Schedule of Fees with a view to ensuring that fees are not a barrier to individuals' right of access and that they provide reasonable compensation for substantial costs incurred by public bodies in responding to complex requests.

19. Amend s. 75 of FIPPA to provide an automatic fee waiver for applicants when a public body has failed to meet the statutory timeline for responding to access requests.

20. Consider reducing or eliminating fees when records have been completely severed such that, in essence, there are no responsive records because none of the information the applicant is seeking is disclosed.

21. Make fee waivers available as a matter of course, without the applicant having to make a specific request, when there is significant public interest in disclosure.

Privacy

Privacy Management Program

The Information and Privacy Commissioner recommended that new provisions be added to FIPPA that would require public bodies to have essential elements of a privacy management program in place. These elements were characterized as accountability measures that demonstrate the responsible management of personal information.

In her presentation to the Committee on November 18, 2015, the Commissioner identified the following core features of a privacy management program that should be prescribed under FIPPA: appointing somebody to be in charge of privacy within a public body, staff training, privacy policies, and privacy breach response plans.

In her written submission, the Commissioner asserted that such requirements would "set clear expectations for public bodies, establish defined criteria for oversight, and, most importantly, safeguard the personal information of British Columbians by proactively requiring a minimal set of privacy controls." Her specific recommendation reads as follows:

> 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.

The Commissioner made a similar recommendation with respect to privacy management program elements to the Special Committee to Review the *Personal Information Protection Act* and it was supported by that committee. In its 2015 report, it recommended that certain additional elements be added to pre-existing ones already in ss. 4 and 5 of the private sector privacy law. The Commissioner argued that requirements in FIPPA "should meet or exceed the

recommended requirements in PIPA" because citizens often have little to no choice about providing their personal information to public bodies.

Government made a recommendation with respect to a privacy management program in its written submission to the Committee. It submitted that comprehensive consultation should be conducted with impacted public bodies on the implications of a legislated requirement to implement a privacy management program. In particular, consideration should be given to the level of specificity of the amendment and that a higher-level requirement that permits different implementation options may be preferable to a one-size fits all approach.

In a letter to the Chair of the Committee dated March 21, 2016, the Information and Privacy Commissioner explained the scalability of a privacy management program. She stated that the scope of a privacy management program would necessarily shift depending on the nature of the public body, the volume of personal information under its control, and the sensitivity of that information.

Committee Members discussed the Information and Privacy Commissioner's recommendation with respect to a privacy management program. Committee Members considered that such a program would enhance privacy protection and that it would not be unduly onerous or costly for public bodies to implement because it would be scalable depending on the volume and sensitivity of the personal information that a public body has in its custody or control. The Committee agreed with government that it should consult with public bodies regarding the impacts of statutory requirements in relation to a possible privacy management program before bringing forward the necessary amendments to FIPPA.

Recommendation

The Committee recommends to the Legislative Assembly that the provincial government:

22. 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.

Notification for Collection of Employee Information [s. 27(4)]

Section 27 of FIPPA requires public bodies to collect personal information directly from the individual the information is about unless an exception applies. One exception is that indirect collection is permitted where the information is about an employee and the information is necessary for the purposes of managing or terminating an employment relationship between a public body and the employee. Because the collection is indirect, the public body must give notice to the employee unless notification would compromise the availability or accuracy of the information, or an investigation or a proceeding related to the employment of the employee.

In its submission to the Committee, the Canadian Bar Association pointed out that there appears to be a drafting error in that notice is required for indirect collection of employee information, but is not required for direct collection of employee information. In its view, this inconsistency can make it impossible for public bodies to conduct an investigation. For example, the employer would not have to notify the employee when it is interviewing witnesses but would have to notify the employee when it is reviewing internet logs (which could give the employee an opportunity to tamper with them).

The Information and Privacy Commissioner indicated that she does not agree that the provision needs to be amended. In her view, the appropriate means to address the concern raised by the Canadian Bar Association is to prospectively notify all employees that covert collection may occur in certain limited circumstances where it is necessary. Employers should advise all employees that, during the course of their employment, personal information may be collected covertly during an employer investigation into alleged employee wrongdoing. This prospective notification would satisfy the requirements of FIPPA without compromising any specific investigation.

The Committee carefully considered the submission of the Canadian Bar Association and agreed with its proposal that FIPPA be amended to permit a public body to not notify the employee that it is collecting their personal information, either indirectly or directly, for the purposes of managing or terminating the employment relationship where it is reasonable to expect that doing so would compromise (a) the availability or the accuracy of the information, or (b) an investigation or a proceeding related to the employment of the employee.

Recommendation

The Committee recommends to the Legislative Assembly that the provincial government:

23. Amend FIPPA to permit a public body to not notify the employee that it is collecting their personal information, either indirectly or directly, for the purpose of managing or terminating the employment relationship, where it is reasonable to expect that doing so would compromise (a) the availability or the accuracy of the information, or (b) an investigation or a proceeding related to the employment of the employee.

Data Security Requirements (s. 30)

Section 30 of FIPPA requires a public body to protect personal information in its custody or under its control by making reasonable security arrangements against such risks as unauthorized access, collection, use, disclosure, or disposal.

The College of Registered Nurses of BC suggested that a higher standard than reasonableness should be imposed in a regulation. The Committee also received recommendations to impose and define certain aspects of security arrangements. The National Association for Information Destruction – Canada suggested that FIPPA should specifically require destruction of information when it is no longer needed and that "destruction" be defined. Similarly, the City of Surrey suggested adding a definition of "securely destroyed."

The Committee concluded that the reasonableness standard in terms of security arrangements is appropriate given rapidly evolving technology and industry standards and that what is reasonable depends on the circumstances. The standard varies depending on the amount and sensitivity of personal information being protected and the best security

measures, such as encryption, that are available at the time. It would therefore be difficult to specify this variable and fluid standard of reasonableness in a regulation.

In terms of requirements and definitions in relation to destruction, the Committee concluded that secure destruction is an essential aspect of reasonable security arrangements and that a specific requirement is not necessary.

Limits on Disclosure

Disclosure Outside Canada (s. 33.1)

Section 33.1 of FIPPA authorizes public bodies to disclose certain personal information inside or outside Canada under certain conditions. For example, disclosure is permitted with the consent of the individual the personal information is about when the consent is given in the prescribed manner. Pursuant to s. 33.1(3) of FIPPA, disclosure outside Canada may also be permitted in specific cases or specified circumstances by ministerial order.

The Committee received two recommendations for additional permitted disclosures outside Canada. The Information and Privacy Commissioner recommended that public bodies be permitted to post non-statutory investigation or fact-finding reports on-line where the public interest in disclosure outweighs the privacy interests. FutureBook Printing Inc. recommended that public bodies be permitted to temporarily disclose limited, non-sensitive student information outside Canada for the sole purpose of yearbook production and printing through a ministerial order under s. 33.1(3).

The College of Registered Nurses of BC made a general recommendation that ss. 33.1 and 33.2 be simplified. They are long, complex, and difficult to understand and interpret, resulting in costly fees for legal advice.

In considering these recommendations, the Committee noted that it was only the recommendation of the Information and Privacy Commissioner that would require adding a new provision to FIPPA. In keeping with its other recommendations with respect to proactive disclosure earlier in this report, the Committee agreed that there should be proactive disclosure of non-statutory investigations and fact-finding reports, and that any provision that prohibits such disclosures should be amended to permit them.

Recommendation

The Committee recommends to the Legislative Assembly that the provincial government:

24. Amend s. 33.1(1) to permit public bodies to post non-statutory investigation or fact-finding reports on-line where the public interest in disclosure outweighs the privacy interests.

Disclosure Inside Canada (s. 33.2)

Section 33.2 of FIPPA permits public bodies to disclose personal information inside Canada in certain circumstances. Sara Levine, Q.C., advocated an amendment that would permit hospitals to disclose patient names to representatives of religious organizations on the basis of implied consent where patients have provided information about religious affiliation.

Section 33.2(l) of FIPPA permits a public body to disclose personal information to another public body if the information is necessary for the purposes of planning or evaluating a program or activity of a public body.

The Information and Privacy Commissioner recommended adding a de-identification requirement to this authorization so that only de-identified personal information could be disclosed for the purposes of planning or evaluating a program or activity of a public body. The Commissioner pointed out that this would be consistent with a recommendation of the previous statutory review committee in 2010 that only de-identified data would be used. In the Commissioner's view, the authorization as is potentially creates unnecessary privacy risks for the individuals whose personal information is used.

The previous statutory review committee recommended that government amend FIPPA 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.

In their deliberations, Committee Members considered the thoughtful recommendation to amend s. 33.2 but felt that a new provision regarding implied consent may not be necessary in this instance when patients could presumably give their express consent to the disclosure in most cases. The Committee concluded that such a narrow and specific exception in FIPPA may not be warranted.

In relation to the disclosure of personal information for the purpose of planning or evaluating a program or activity of a public body under s. 33.2(l), Committee Members recognized the importance of planning or evaluating a program or activity of a public body as well as the importance of minimizing privacy risks in doing so. The Committee thought that planning or evaluating could be accomplished by using de-identified data, and therefore concluded that FIPPA should be amended to permit only the disclosure of de-identified data for that purpose.

Recommendation

The Committee recommends to the Legislative Assembly that the provincial government:

25. Amend s. 33.2(l) of FIPPA to permit only de-identified personal information to be disclosed for the purposes of planning or evaluating a program or activity of a public body.

Privacy Impact Assessments (s. 69)

Section 69 of FIPPA requires a public body to conduct a privacy impact assessment during the development of a proposed enactment, system, project, program, or activity. The head of a ministry must conduct a privacy impact assessment in accordance with the directions of the minister responsible for FIPPA.

In its written submission to the Committee, government recommended that s. 69 be amended to clarify when and how a privacy impact assessment must be completed and to provide clearer authority for the minister to issue directions on conducting and submitting privacy impact assessments.

The Information and Privacy Commissioner indicated that she would support such amendments.

The Committee discussed the importance of completing privacy impact assessments in the early stages of all proposed initiatives that involve the collection, use, or disclosure of personal information. A privacy impact assessment identifies the privacy risks of the proposed initiative and the steps that will be taken to mitigate them. The Committee supported strengthening provisions in FIPPA that require public bodies to complete privacy impact assessments.

Recommendation

The Committee recommends to the Legislative Assembly that the provincial government:

26. Amend s. 69 of FIPPA to clarify and strengthen requirements with respect to privacy impact assessments.

Oversight of the Information and Privacy Commissioner

Destruction of Records

Section 42(1) of FIPPA gives the Commissioner the authority to conduct investigations and audits to ensure compliance with any provision of FIPPA. In her written submission to the Committee, the Information and Privacy Commissioner recommended expanding this authority by granting her office legislative authority to investigate whether a record has been destroyed contrary to records management rules. This recommendation was supported by the BC Civil Liberties Association, CUPE BC Division, and the Local Government Management Association.

Currently, the Information and Privacy Commissioner has the authority to investigate if the alleged destruction of records occurred after an access request was made but has no authority in the absence of an access request.

The Alberta Information and Privacy Commissioner has this broader oversight authority with respect to the destruction of records pursuant to s. 53 of the Alberta *Freedom of Information and Protection of Privacy Act*. It gives the Information and Privacy Commissioner the power to:

> conduct investigations to ensure compliance with any provision of this Act or compliance with rules relating to the destruction of records
>
> i. set out in any other enactment of Alberta, or
>
> ii. 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 Loukidelis report includes a recommendation that government should give serious consideration to introducing legislation consistent with s. 53 of the Alberta *Freedom of Information and Protection of Privacy Act*.

In British Columbia, the adoption of such a provision would give the Information and Privacy Commissioner oversight over compliance with rules related to the destruction of records in the *Information Management Act*, any other Act, and in rules governing local public bodies (i.e. municipalities, health authorities, Community Living BC, universities, school boards, and professional regulatory bodies). Presumably the intent is to ensure compliance with information schedules made pursuant to the *Information Management Act* that apply to a class

of government information or any other analogous recordkeeping requirements that apply to local public bodies insofar as they prohibit the destruction of records.

Under s. 19(5) of the *Information Management Act* the head of each government body must ensure that no government information held by the government body is disposed of, except in accordance with an information schedule or an approval by the Chief Records Officer where no information schedule exists. In its submission, government said that independent oversight could create confusion and potential conflict, as it would result in two officers responsible for overseeing different or overlapping aspects of information management. In its view, oversight of the destruction of records would fit better in the *Information Management Act*, which governs the entire life-cycle of information, including its eventual destruction.

In their deliberations, Committee Members discussed the merits of independent oversight and the need to maintain public trust and confidence in information management and in the FOI process. The Committee therefore felt that the Information and Privacy Commissioner should have the authority to investigate allegations of unauthorized destruction of records within public bodies.

Recommendation

The Committee recommends to the Legislative Assembly that the provincial government:

27. Amend s. 42 of FIPPA to expand the Information and Privacy Commissioner's oversight by granting the Commissioner the jurisdiction to review matters or allegations of unauthorized destruction of records within public bodies.

Data-linking Initiatives

Specific provisions with respect to data linking were added to FIPPA as part of the 2011 package of amendments. Section 69 of FIPPA was amended to include, among other things, a requirement that privacy impact assessments in relation to data-linking initiatives must be submitted to the Information and Privacy Commissioner for review and comment. Data-linking initiatives within the health sector are excluded from this requirement.

The Information and Privacy Commissioner submitted that her oversight of data-linking initiatives needs to be expanded because the definition of data-linking initiatives is too narrow and because privacy risks associated with the carve-out for the health sector have not been addressed by government. She made the following recommendation as to how the definition of "data-linking" should be amended:

> 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.

With respect to the carve out from data linking requirements for the health sector, the Information and Privacy Commissioner recommended the repeal of s. 36.1(2) to remove the exemption of the health care sector from the data-linking oversight provisions of FIPPA.

In their presentation to the Committee on November 18, 2016, government officials stated that they recognized that the narrow definition of "data-linking initiative" failed to capture the types of activities which should be subject to the Information and Privacy Commissioner's oversight. Government advised that it has identified data-linking provisions as a key legislative amendment and that it had embarked on extensive consultation with the Office of the Information and Privacy Commissioner, and had developed a new legislative scheme that will meet the needs of all stakeholders.

The Committee recognized the intention of the Legislative Assembly in 2011 to have independent oversight of data-linking initiatives except with respect to data-linking initiatives within the health sector. The Committee endorsed government's proposal to correct the narrow definition that prevented the Information and Privacy Commissioner from exercising the level of oversight that was intended.

With respect to the carve-out for the health sector, the Committee concluded that government should address the privacy risks associated with data-linking initiatives within the health sector and consult with the Information and Privacy Commissioner on how best to do so.

Recommendations

The Committee recommends to the Legislative Assembly that the provincial government:

28. Amend the definition for "data-linking" in Schedule 1 of FIPPA to define data-linking as the linking or combining of datasets 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 datasets that was originally obtained or compiled, and any purposes consistent with that original purpose.

29. Address the privacy risks associated with data-linking initiatives within the health sector in consultation with the Information and Privacy Commissioner.

Processes

Parts 4 and 5 of FIPPA provide for two types of public appeals to the Office of the Information and Privacy Commissioner – complaints and requests for review. Under s. 42(2), a person may file a complaint that a public body is in contravention of FIPPA, and under s. 52(1), a person can request that the Information and Privacy Commissioner review the outcome of a request made to a public body.

The Information and Privacy Commissioner submitted that the distinction between complaints and requests for review is unnecessary, confusing, and burdensome because individuals require assistance to navigate them. She therefore brought forward the same recommendation that had been made in the past by her predecessors in two previous statutory reviews, and that had been endorsed by both statutory review committees. In reports in 2004 and 2010, the two previous statutory review committees recommended that FIPPA be amended to combine the complaint process and the review and inquiry process into a unitary process for the Commissioner to investigate, mediate, inquire into, and make orders about complaints respecting decisions under FIPPA or other allegations of non-compliance with FIPPA.

In their presentation to the Committee on November 18, 2016, government officials identified one of its key legislative amendments as proposed changes that would 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. 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.

In their deliberations, Committee Members noted that the Information and Privacy Commissioner and her predecessors, as well as two previous statutory review committees, had recommended amendments to FIPPA that would create a unitary process and harmonize the complaint, review, and inquiry process, and that government is prepared to bring forward the necessary amendments. Members recognized that the problems experienced by the Office of the Information and Privacy Commissioner as a result of two separate avenues for public appeals were longstanding, and concluded that the proposed changes would create a more efficient overall process.

Recommendation

The Committee recommends to the Legislative Assembly that the provincial government:

30. 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.

Enforcement of FIPPA

Unauthorized Destruction of Records

The Committee received a number of submissions on the issue of offences and penalties for the unauthorized destruction of records, including from the Information and Privacy Commissioner, the BC Freedom of Information and Privacy Association, Stanley Tromp, BC Civil Liberties Association, the Centre for Law and Democracy, CUPE BC Division, Douglas Ash, and Greig Hull. The Canadian Taxpayers Federation, supported by separate submissions from 126 individuals, advocated tougher penalties to ensure that government agencies follow the law and provide information in a timely fashion, including fines and/or incarceration, for willfully hiding information from the public.

The Information and Privacy Commissioner recommended that an explicit offence of the willful unauthorized destruction of records should be written into FIPPA. In her written submission, she identified precedents in Alberta and Ontario where the unauthorized destruction of records is an offence.

The Loukidelis report included a recommendation that government give serious consideration to introducing legislation, consistent with s. 92(1) of the Alberta *Freedom of Information and Protection of Privacy Act*, that would make it an offence to destroy a record, or direct or assist anyone else in doing so with the intent to evade a request for access to the records.

Sections 92 (e) and (g) of the Alberta statute provide that the unauthorized alteration or destruction of records with the intent to evade a request for access is an offence. The provisions read as follows:

> 92. A person must not willfully
>
> (e) alter, falsify or conceal any record, or direct another person to do so, with the intent to evade a request for access to the record,
>
> (g) destroy any records subject to this Act, or direct another person to do so, with the intent to evade a request for access to the records.

Ontario's Act was recently amended to add a similar provision:

> 61 (1) No person shall,

(c.1) alter, conceal or destroy a record, or cause any other person to do so, with the intention of denying a right under this Act to access the record or the information contained in the record.

BC's private sector privacy law, the *Personal Information and Protection of Privacy Act*, includes the offence of destruction of personal information with the intent to evade an access request. It reads as follows:

56 (1) an organization or person commits an offence if the organization or person …

(b) disposes of personal information with an intent to evade a request for access to the personal information.

In its written submission to the Committee, government advised that its position with respect to the destruction of records is that government should monitor and evaluate the efficacy of existing training and compliance programs and consider increased oversight and penalties in the *Information Management Act* if needed. Requirements for government employees respecting information management practices are set out in the *Appropriate Use of Government Information and Information Technology Policy* which is supported by the Standards of Conduct.

The Committee carefully considered the recommendations of the current and former Information and Privacy Commissioner that it should be an offence to destroy a record with the intention to evade an access request. Members noted there was a measure of public support for such a provision as evidenced by the number of submissions it had received from individuals on this issue. The Committee agreed that it should be an offence under FIPPA to destroy a record with the intention to evade an access request as it is under Alberta and Ontario access to information laws.

Recommendation

The Committee recommends to the Legislative Assembly that the provincial government:

31. Amend FIPPA to make the alteration, concealment, or destruction of records with the intention of denying access rights under FIPPA an offence under FIPPA.

Privacy Protection Offence (s. 74.1)

Section 74.1 of FIPPA sets out a number of offences under FIPPA, including the unauthorized disclosure of personal information. The Information and Privacy Commissioner recommended making the unauthorized collection and use of personal information also an offence under FIPPA. In her presentation to the Committee on November 18, 2015, she characterized such an offence as the "snooping offence." It would mean that sanctions are available for improper access to personal information in any electronic database system held by a public body.

Public sector privacy laws, including health information privacy laws, in several provinces in Canada contain a general offence for the unauthorized collection, use, or disclosure of personal information. For example, s. 92(1)(a) of Alberta's *Freedom of Information and Privacy Act* reads as follows:

> 92 .(1) A person must not willfully
>
> (a) collect, use or disclose personal information in contravention of Part 2

The Committee agrees that the collection, use, and disclosure of personal information contrary to the privacy protective provisions of FIPPA should be an offence. This would provide an incentive for compliance as well as an appropriate sanction for an intentional breach of privacy.

Recommendation

The Committee recommends to the Legislative Assembly that the provincial government:

32. Amend s. 74.1 of FIPPA to make the unauthorized collection, use, and disclosure of personal information in contravention of Part 3 of FIPPA an offence under FIPPA.

Penalties (ss. 74 and 74.1)

Sections 74(5) and 74.1(5) of FIPPA set out penalties for general and privacy protection offences under FIPPA. Section 74(5) provides for a fine of up to $5000 where a person makes a false statement, misleads, or obstructs the Information and Privacy Commissioner in the

performance of her duties or fails to comply with an order of the Information and Privacy Commissioner. Section 74.1 sets out a number of privacy offences, including unauthorized disclosure (a contravention of s. 30.4), failure to notify the head of the public body of an unauthorized disclosure (a contravention of s. 30.5), and storing or accessing personal information outside Canada (a contravention of s. 30.1). An individual is liable to a fine of up to $2000, a service provider to a fine of up to $25,000, and a corporation to a fine of up to $500,000.

A number of participants in the Committee's consultation process recommended increasing the maximum amount of fines that may be levied against individuals. The Information and Privacy Commissioner recommended that penalties for offences committed by individuals should be raised to a maximum of $50,000 for both general and privacy offences. She argued that:

> British Columbia has some of the weakest penalties in Canada for individuals who commit offences under public sector privacy law. This undermines the role that penalties play as an incentive for compliance, suggesting that the government does not take access and privacy seriously.

The following comparative information was included in her written submission:

> Penalties are up to $50,000 in Alberta's *Health Information Act*, Saskatchewan's *Health Information Protection Act*, and both Manitoba's *Freedom of Information and Protection of Privacy Act* and its *Personal Health Information Act*. Penalties are up to $25,000 in the Yukon's *Health Information Privacy and Management Act* and up to $10,000 in Alberta's *Freedom of Information and Protection of Privacy Act*, PEI's *Freedom of Information and Protection of Privacy Act*, and Newfoundland and Labrador's *Access to Information and Protection of Privacy Act* and its *Personal Health Information Act*.

The BC Civil Liberties Association pointed out that a fine of up to $5000 is far below what other jurisdictions have implemented as a meaningful deterrent, and that fines of up to $50,000 are permitted in Alberta, Saskatchewan, and Manitoba. Stanley Tromp said that the amount of fines should be raised to a maximum of $50,000, and that the fine for obstructing the Information and Privacy Commissioner should be $10,000. Many individuals who made submissions to the Committee also advocated tougher penalties for not complying with FIPPA requirements.

Stanley Tromp's position is that the penalties should be the same as in the federal *Access to Information Act* -- a maximum fine of $10,000 and a 2 year prison term for any person destroying, altering, or concealing a record. The Canadian Taxpayers Federation, and the many

individuals supporting its position, stated there should be penalties, fines, and/or prison time for willfully hiding information from the public. However, the Centre for Law and Democracy was of the view that jail terms are usually not necessary.

Another aspect to the penalties that should be in place is the discipline of government employees for the unauthorized destruction of records. The recommendation was made in the Loukidelis report that government should make such policy and practice changes as are necessary to ensure that any employee appointed under the *Public Service Act* who destroys a record, or directs or assists anyone else in doing so, with the intent to evade a request for access to the record is subject to discipline up to and including dismissal for cause.

In its written submission to the Committee, government said its employees who fail to comply with information management standards may be subject to disciplinary action up to and including dismissal. This includes employees who willfully destroy government information that should not be destroyed (whether or not the information is the subject of an access request). As previously mentioned, government said that it will consider whether increased oversight and penalties are needed, including adding increased oversight authority and penalties to the *Information Management Act*.

Recommendations

The Committee recommends to the Legislative Assembly that the provincial government:

33. Increase the maximum amount of fines for general offences from $5000 to $10,000 and increase the maximum amount of fines for privacy offences committed by individuals to $25,000.

34. Institute a fine of up to $10,000 for the offence of destroying, altering, or concealing a record with the intention of denying access rights under FIPPA.

General

Require Corrections to be Made (s. 29)

Pursuant to s. 29 of FIPPA, individuals have the right to request public bodies to make corrections to the personal information about them that public bodies have in their custody or control. The Information and Privacy Commissioner recommended that public bodies be required to correct personal information of an individuals at his/her request if the public body is satisfied on reasonable grounds that the personal information should be corrected.

The Committee considered that an amendment to FIPPA that would require public bodies to correct personal information at the request of an individual that the information is about, if there are reasonable grounds for the public do so, is in the public interest. It would strengthen the right to request a correction and make it more effective and meaningful.

Recommendation

The Committee recommends to the Legislative Assembly that the provincial government:

35. Amend FIPPA to require public bodies to correct personal information at the request of an individual the information is about if there are reasonable grounds for the public body to do so.

Provisions that Prevail Over FIPPA

Section 80(2) of FIPPA provides that a report submitted by a special committee to review FIPPA may include any recommended amendments to FIPPA or any other Act.

In British Columbia, there are 43 separate pieces of legislation that contain provisions that override FIPPA. These range from the *Child, Family and Community Service Act* to the *Local Government Act* and the *Representative for Children and Youth Act*.

In their submissions, the Information and Privacy Commissioner, the BC Freedom of Information and Privacy Association, the BC Civil Liberties Association, the Centre for Law and Democracy, and the BC Public Interest Advocacy Centre expressed concerns regarding the number of provisions that prevail over FIPPA, and recommended that they be reviewed. As stated in the submission of the Information and Privacy Commissioner, "Growth in the list of

provisions in statutes that prevail over FIPPA diminishes the access rights of individuals in BC." The Centre for Law and Democracy said that government should make sure that the exceptions protect legitimate interests and are subject to a harms test and a public interest override. The BC Public Interest Advocacy Centre suggested aligning the exemptions with the objectives of FIPPA in order to reduce the disparity between the accessibility of public records subject to, or exempt from, FIPPA.

The Information and Privacy Commissioner recommended that the statutory review of FIPPA by a special committee of the Legislature include a review of those provisions that prevail over FIPPA. As a mechanism for that regular statutory review, she recommended that the provisions be listed in a schedule to FIPPA.

In their deliberations, Committee Members recognized the need to review the significant number of provisions in other legislation that prevail over FIPPA and thought that such a review was in the Committee's mandate pursuant to s. 80(2) of FIPPA. However, given the complexity of that task and the amount of time that would be required to conduct a thorough review, the Committee concluded that the review should be conducted by a separate committee of the Legislature struck for that specific purpose. The Committee agreed that it could be part of the next statutory review provided that an adequate amount of time is allocated by the Committee for that specific task and consultations are expanded as necessary to focus on the access and privacy issues raised by each of the overrides.

Recommendation

The Committee recommends that the Legislative Assembly:

36. Appoint a special committee to conduct a review of the existing overrides of FIPPA and make recommendations to the Legislative Assembly as to whether they should be amended or repealed.

Sector-Specific Privacy Legislation

Currently in BC, personal information in the custody or control of the Ministry of Health and health authorities is generally governed under FIPPA, while personal information in the custody or control of private practices of health professionals is generally governed under the

Personal Information Protection Act. There are also other pieces of health legislation that apply to specific types of personal health information, such as the *E-Health (Personal Health Information Access and Protection of Privacy) Act* which applies to personal health information of the ministry or health authorities contained in designated databases and provisions in the *Public Health Act* that apply to personal health information related to public health matters such as the reporting of disease.

The Information and Privacy Commissioner recommended to the Committee that government enact new comprehensive health information privacy law and referred to previous recommendations she had made in that regard in a 2014 report titled *Prescription for Legislative Reform: Improving Privacy Protection in BC's Health Sector*. In that report, she described the existing patchwork of health information legislation that applies to personal information collected for the purpose of delivering health care, and recommended that it be replaced with a stand-alone health information privacy law such as exists in other provinces. In the Commissioner's view, the patchwork is opaque and complex and is challenging for individuals, health care professionals, administrators, and researchers to navigate. In her submission to the Committee, she said that, "This is administratively inefficient for the health sector, is unnecessarily cumbersome for researchers, and ultimately puts the privacy of individuals at potential risk of harm."

The Information and Privacy Commissioner made a similar recommendation to the Special Committee to Review the *Personal Information Protection Act* in 2014. In its 2015 report, that Committee recommended that "the provincial government develop a new health information privacy law that is consistent with laws in other jurisdictions in Canada."

Surrey School District #36 recommended education-specific privacy protective provisions. It submitted that the education sector requires more robust and distinct language and that the storage of personal data by educational bodies warrants separate legislation, or the addition of sector-specific clauses or sections to the existing legislation.

In their deliberations, Committee Members recognized that the health sector is unique and discussed the complexities of preparing a new stand-alone health information privacy law. It would involve a considerable amount of time, expertise, and resources given that it would require extensive consultations within the health sector, including internally within the Ministry of Health, with health authorities, health professionals, health researchers, and other organizations delivering health care, as well as with patients, privacy advocates, and the Information and Privacy Commissioner. Difficult decisions would need to be made on many significant health privacy issues such as statutory requirements for privacy and security frameworks for electronic health record systems, authorities for data flows among health care

providers, and appropriate access to data for health research. Committee Members agreed, however, that given that the delivery of health care in a publicly-funded system involves the collection, use, and disclosure of highly sensitive personal health information about almost every individual in BC, it is essential that it be protected adequately and that there are proper authorities for necessary data flows within the system, to health researchers, and for other health-related purposes.

The Committee concluded that a stand-alone health privacy law is a critically important initiative that should be considered by government as a priority.

Identifying whether there is a need for special provisions in FIPPA that would apply to the education sector should also be a priority. This would require extensive consultations with stakeholders within the education sector, including internally within the Ministry of Education as well as with teachers, administrators, school trustees, and parents.

Recommendations

The Committee recommends to the Legislative Assembly that the provincial government:

37. Enact new stand-alone health information privacy law at the earliest opportunity.

38. Consult with stakeholders in the education sector as to whether there is a need for special provisions in FIPPA that are tailored to the education sector.

Establish Provincial Oversight

As previously discussed in this report, the Information and Privacy Commissioner, an independent statutory officer of the Legislature, has oversight responsibilities for the implementation of FIPPA. Stephen Bohus advocated that there also be provincial oversight so that government could audit public bodies and appoint teams to rectify issues where there are systemic problems.

The Committee was of the view that provincial oversight would overlap with the mandate of the Office of the Information and Privacy Commissioner and therefore is not necessary.

Create the Role of a Chief Privacy and Access Officer in Government

In their joint written submission, Ryan Berger and Sara Levine, Q.C., recommended that the position of a single, senior chief privacy and access officer in government be established under FIPPA.

> We submit that the creation of the role of a Chief Privacy and Access Officer who is granted some authority and reports to the minister, would promote advancement of internal compliance programs enabling government to take into account their particular operational realities, facilitate flexibility and better ensure compliance.
>
> It is a cliché that what gets measured, gets done but there is no doubt that measuring, prioritizing and ensuring senior level oversight, public reporting, and accountability, would promote government's understanding, and compliance with, consistent standards of privacy and information access management. A Chief Privacy and Access Officer, responsible for acting independently but reporting to the minister, would ensure that government demonstrates its intention to be accountable for information access and privacy governance. Demonstrable efforts to increase accountability would promote and enhance public trust.

The previous statutory review committee recommended the appointment of a government Chief Privacy Officer because of the need to educate ministries about what they can and cannot do in regard to privacy matters.

The Committee noted that the position of Chief Records Officer has been established under the *Information Management Act*. The position of a chief privacy and access officer could complement that position by ensuring that there would be similar corporate oversight and guidance to all ministries in relation to access to records. Committee Members felt that a senior level Chief Privacy and Access Officer would provide leadership and accountability for improving the FOI process. Given the potential scope of privacy breaches involving electronic records and rapidly evolving industry standards for data security, privacy protection should be a high priority in government.

Recommendation

The Committee recommends to the Legislative Assembly that the provincial government:

39. Establish the position of Chief Privacy and Access Officer within government.

Summary of Recommendations

Major Recommendations

Proactive Disclosure

1. Amend FIPPA and initiate proactive disclosure strategies to reflect the principle that information that is in the public interest should be proactively disclosed, subject to certain limited and discretionary exceptions that are necessary for good governance and to protect personal information. Among other things, this could be accomplished by:
    - strengthening s. 25(1) to remove the requirement of temporal urgency;
    - establishing a publication scheme that would apply to all public bodies, that includes, among other things, mandatory proactive disclosure of those records listed in s. 13(2)(a) to (n); and
    - developing a system within government to proactively disclose the calendar information of ministers and senior officials that would be disclosed in response to an access request.

Duty to Document

2. Add a duty to document to FIPPA.

Information Management in Government

3. Make all obligations related to the entire life-cycle of government records part of a cohesive and robust information management scheme; and

4. Ensure that archiving is a high priority.

Data Sovereignty

5. Retain the data sovereignty requirement in s. 30.1 of FIPPA.

Application of FIPPA

6. Extend the application of FIPPA to any board, committee, commissioner, panel, agency or corporation created or owned by a public body and all the members or officers of which are appointed or chosen by or under the authority of that public body; and

7. Consider designating all publicly-funded health care organizations as public bodies under FIPPA.

FOI Process

8. Reduce the timeline in which a public body must respond to an access request from 30 business days to 30 calendar days.

9. Review other timelines established in FIPPA with a view to reducing them in order to promote the efficiency and timeliness of the FOI process.

10. Amend section 4(1) of FIPPA to establish that an applicant who makes a formal access request has the right to anonymity.

Mandatory Breach Notification and Reporting

11. Add a mandatory breach notification and reporting framework to FIPPA that 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 the 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 or the public; and
    - a requirement that public bodies document privacy breaches and decisions about notification and reporting.

Other Recommendations

Access

Duty to Assist

12. Amend s. 6 of FIPPA to add a specific requirement for public bodies to make the contact information of the person responsible for ensuring compliance available to the public.

Cabinet Confidences

13. Amend s. 12 of FIPPA to permit the Cabinet Secretary to disclose to an applicant information that would reveal the substance of deliberations of the Executive Council or any of its committees where the Cabinet Secretary is satisfied that the public interest in the disclosure of the information outweighs the reason for the exception.

Personal Privacy

14. Consider initiating a review of whether a parent of a child who was in care should have access to personal information about their deceased child.

Policy Advice or Recommendations

15. Amend s. 13(1) of FIPPA to clarify that the discretionary exception for "advice" or "recommendations" does not extend to facts upon which they are based; or for factual, investigative or background material; or for the assessment or analysis of such material; or for professional or technical opinions.

Legal Advice

16. Amend s. 14 of FIPPA to make it a mandatory exception unless 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.

Law Enforcement

17. Consider whether an explicit reference to investigations that are within the mandate of a professional regulatory body should be added to the definition

of "law enforcement" in Schedule 1 so that a professional regulatory body may refuse to disclose information that may harm an investigation.

Fees

18. Review the Schedule of Fees with a view to ensuring that fees are not a barrier to individuals' right of access, and that they provide reasonable compensation for substantial costs incurred by public bodies in responding to complex requests.

19. Amend s. 75 of FIPPA to provide an automatic fee waiver for applicants when a public body has failed to meet the statutory timeline for responding to access requests.

20. Consider reducing or eliminating fees when records have been completely severed such that, in essence, there are no responsive records because none of the information the applicant is seeking is disclosed.

21. Make fee waivers available as a matter of course, without the applicant having to make a specific request, when there is significant public interest in disclosure.

Privacy

Privacy Management Program

22. 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.

Notification for Collection of Employee Information

23. Amend FIPPA to permit a public body to not notify the employee that it is collecting their personal information, either indirectly or directly, for the purpose of managing or terminating the employment relationship, where it is reasonable to expect that doing so would compromise (a) the availability or the accuracy of the information, or (b) an investigation or a proceeding related to the employment of the employee.

Disclosure Outside Canada

24. Amend s. 33.1(1) of FIPPA to permit public bodies to post non-statutory investigation or fact-finding reports on-line where the public interest in disclosure outweighs the privacy interests.

Disclosure for Planning or Evaluating a Public Body

25. Amend s. 33.2(l) of FIPPA to permit only de-identified personal information to be disclosed for the purposes of planning or evaluating a program or activity of a public body.

Privacy Impact Assessments

26. Amend s. 69 of FIPPA to clarify and strengthen requirements with respect to privacy impact assessments.

Oversight of the Information and Privacy Commissioner

Unauthorized Destruction of Records

27. Amend s. 42 of FIPPA to expand the Information and Privacy Commissioner's oversight by granting the Commissioner the jurisdiction to review matters or allegations of unauthorized destruction of records within public bodies.

Data-Linking Initiatives

28. Amend the definition for "data-linking" in Schedule 1 of FIPPA to define data-linking as the linking or combining of datasets 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 datasets that was originally obtained or compiled, and any purposes consistent with that original purpose.

29. Address the privacy risks associated with data-linking initiatives within the health sector in consultation with the Information and Privacy Commissioner.

Unitary Process

30. 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.

Enforcement of FIPPA

Unauthorized Destruction of Documents

31. Amend FIPPA to make the alteration, concealment, or destruction of records with the intention of denying access rights under FIPPA an offence under FIPPA.

Privacy Protection Offence

32. Amend s. 74.1 of FIPPA to make the unauthorized collection, use, and disclosure of personal information in contravention of Part 3 of FIPPA an offence under FIPPA.

Penalties

33. Increase the maximum amount of fines for general offences from $5000 to $10,000 and increase the amount of fines for privacy offences committed by individuals to up to $25,000.

34. Institute a fine of up to $10,000 for the offence of destroying, altering, or concealing a record with the intention of denying access rights under FIPPA.

General

Correction

35. Amend FIPPA to require public bodies to correct personal information at the request of an individual the information is about if there are reasonable grounds for the public body to do so.

Review of Provisions that Prevail over FIPPA

36. Appoint a special committee to conduct a review of the existing overrides of FIPPA and make recommendations to the Legislative Assembly as to whether they should be amended or repealed.

Sector-Specific Privacy Legislation

37. Enact new stand-alone health information privacy law at the earliest opportunity.

38. Consult with stakeholders in the education sector as to whether there is a need for special provisions in FIPPA that are tailored to the education sector.

Chief Privacy and Access Officer

39. Establish the position of Chief Privacy and Access Officer within government.

Appendix A: List of Witnesses and Written Submissions

Witnesses

AMS Student Society of UBC Vancouver, Jude Crasta (Oct 16, 2015, Vancouver)
BC Freedom of Information and Privacy Association, Vincent Gogolek (Oct 16, 2015, Vancouver)
Stephen Bohus (Oct 16, 2015, Vancouver; Nov 9, 2015, Vancouver)
Robert Botterell (Nov 9, 2015, Vancouver)
Canadian Internet Policy and Public Interest Clinic (CIPPIC), Tamir Israel (Nov 18, 2015, Victoria)
Canadian Union of Public Employees Local 116, Roger De Pieri, David Lance, Rachel Champagne (Nov 9, 2015, Vancouver)
Centre for Law and Democracy, Michael Karanicolas (Oct 16, 2015, Vancouver)
College of Registered Nurses of BC, Cynthia Johansen, Orvin Lau
David DeCosse (Nov 9, 2015, Vancouver)
Lisa Fraser (Nov 9, 2015, Vancouver)
FutureBook Printing, Inc., Dana Felske (Nov 9, 2015, Vancouver)
Sara Levine, Q.C., Ryan Berger (Nov 9, 2015, Vancouver)
Laura Millar (Nov 9, 2015, Vancouver)
Owen Munro, James Smith (Nov 18, 2015, Victoria)
Regional District of Central Kootenay, Bronwen Bird (Nov 18, 2015, Victoria)
Joan L. Rush (Nov 9, 2015, Vancouver)
Paul Schwartz (Nov 9, 2015, Vancouver)
The Ubyssey, Will McDonald (Nov 9, 2015, Vancouver)
Stanley Tromp (Nov 9, 2015, Vancouver)
University of British Columbia; Research Unversities' Council of British Columbia, Paul Hancock, Larry Carson (Nov 9, 2015, Vancouver)
Vancouver Coastal Health Authority, Steven Tam (Nov 9, 2015, Vancouver)
Gordon Watson (Oct 16, 2015, Vancouver)
West End Neighbours, Virginia A. Richards (Nov 9, 2015, Vancouver)
Rob Wipond (Nov 18, 2015, Victoria)

Written Submissions:

L.A. Abraham
James Allen
James Andrews
Timo Annala
Bruce Apperloo
Chris Armstrong
Douglas Ash
Mike Bacinschi
Gordon Ballard
BC Government and Service Employees' Union (BCGEU), Simon Kelly
BC Public Interest Advocacy Centre, Tannis Braithwaite
BC School Superintendents Association; BC Association of School Business Officials, Sherry Elwood, Kelvin Stretch
BCNET, Bala Kathiresan
Celena Benndorf
Board of Education, School District No. 46 (Sunshine Coast), Betty Baxter
John Boer
Blain Borneman
Dan Bowes
BC Civil Liberties Association, Micheal Vonn
BC Lottery Corporation, Robert Connolly
Diane Brown
Ron Bruce
Andrew Bryant
Mike Butterfield and Julia Vertone
Canadian Centre for Policy Alternatives, BC Office, Keith Reynolds
Canadian Taxpayers Federation, Jordan Bateman
Canadian Union of Public Employees, BC Division, Paul Faoro
Ron Chambers
Mark Choynowski
Christian Heritage Party of BC; Christian Heritage Party of Canada, Rod Taylor
College of Registered Nurses of BC, Cynthia Johansen
Margriet Coolsma
Sue Cosquer
William Costain
Ken Daniels
Don Davidson
Peter Derviller
Marvin and Pat DeSchryver
Garry Dietrich
Victoria Dobson
Jasbir Singh Dulai
Jeff Durham
John Edwards
Robert Fair
Paul Faoro
Gino Ficociello
Roszan Fiddler
Rick Fijal
Fred Forman
Ray Fortier
Richard Gee
Glen Gerow
Kenneth Godwin
Douglas Golding
Doreen Gowans
Kevin and Mrs Granger-Brown
Aaron Grim
Jim Guillaume
Edward Gullickson
John Hackett
Bruce Hallquist
James Hannah
C. Douglas Henning
Don Herner
Beverley Highton
Gary Hill
Cecile Hilts
Ken Hinton
John Hof

Greig Hull
J.C. Hunter
JoAnn Ingeberg
Insurance Corporation of British Columbia, David Joyce
IntegrityBC, Dermod Travis
Michael James
Cynthia Johansen
Richard Jones
Frederik Jurock
Bala Kathiresan
Rodney Katz
Michael Kelly
Kevin Kerney
Dale Kerr
Judi Kirkland
Lynn Kisilenko
Bernadette Klaibert
Curby Klaibert
Candy Klaudeman
Cassandra Knegt
Olaf Knexevic
Jennifer Kotteleberg
Hilmar Krocke
Ma Kudo
Marilyn Kuss
Dora Kwok
Len and Marlyn Lakes
Ryan LaPalm
Law Society of BC, David Crossin, Q.C.
Douglas Leard
Lisa Lewko
Shannon Leyenhorst
Larry Lloyd
Shaun Lockwood
Sophie Loehrich
Peter Loppe
David Low
Bob Mackin, Jr.
Dan Mancuso
Dale Marcellus
Greig Marshall
Michael McDonald
Neil McGill
Diana McGraw
Callum McGregor
Cathy McLay
Jim McNeil
Gord McOrmond
Richard Meagher
Michelle Menard
James Messmer
Microzip Data Solutions Inc., Axel Krieger
Luanne Morris
National Association for Information Destruction - Canada, Duncan Rayner
Barry Nauss
Norbert Neumann
Vic Nielsen
Michelle Nordeman
Robert Odynski
Terry O'Neill
Deborah Oosterhoff
Bud Oujla
Robert Overland
Colin Parker
Heinz Patzke
Ritchie Po
Charlene Ratzinger
Richard Rickard
Malcolm Roberts
Peter Robson
John Ryan
Joanne Sager
Mark Salter
Sylvia Schell
Barrie Seed
Bill Shumborski
John Smart
Jeannette St. Pierre
Peter Stornebrink
Surrey School District No. 36, Jordan Tinney
Robyn Thornton
Devin Todd

TransLink, Cathy McLay
Stan Turner
United for Life Advocacy Association of BC, John Hof
Larry Uzelman
Valerie van de Wint
Kors van Kreuningen
Vancouver Coastal Health Authority; Fraser Health Authority; Vancouver Island Health Authority; Northern Health Authority; Providence Health Care, C.C. (Kip) Woodward
Celia Vandergugten
Sid Veenbaas
Michael Volansky
Adam Waitzer
WeNeedaLaw.ca, Anna Nienhuis
Greg Wenger
Gordon Widsten
Larry Wierenga
Paul Williams
John F Wilson
Neil Yonson