TABLE OF CONTENTS - APPENDIX A

APPENDIX A

AMENDMENTS TO PROVINCIAL AND TERRITORIAL PRIVACY LAWS IN SUPPORT OF INNOVATION

Most jurisdictions in Canada have, over the years, amended their public sector privacy laws to facilitate information sharing and use of technology in support of innovation by Public Bodies. This appendix outlines these amendments by jurisdiction and the rationale where available.

Explanatory Notes

The provisions marked in red delineate amendments made to the legislation in question.

BC'S FIPPA

During the review of BC's FIPPA in 2010, former Acting Commissioner Fraser made the following recommendations specific to information sharing and the use of technology.[1]

> *2. Government should not proceed with any more data sharing initiatives until a meaningful public consultation process has occurred, and the outcome of that process is an enforceable code of practice for data sharing programs.*[2]
>
> *4. FIPPA should be amended to give the OIPC a statutory mandate to review and approve all data sharing initiatives.*

[1] Submission of the A/Commissioner to the Special Committee to Review the *Freedom of Information and Protection of Privacy Act*, March 15, 2010, A/Commissioner Fraser, located at: https://www.oipc.bc.ca/special-reports/1275.

[2] The data sharing code of practice recommendation stemmed from guidance prepared by the European Union's Information Commissioner's Office, https://ico.org.uk/media/for-organisations/documents/1068/data_sharing_code_of_practice.pdf. In this guidance, two types of data sharing are defined: 1) systematic, routine data sharing where the same data sets are shared between the same organizations for an established purpose, and 2) exceptional, one-off decisions to share data for any of a range of purposes, at page 9. The code contains best practices, designed to assist bodies, including public sector bodies, implement practices around information sharing to better protect privacy. The guidance recommends bodies establish practices to: clarify the legal authority to share personal information; make decisions about whether to share personal information including factors to guide decision making; ensure individuals are informed about the information sharing; evaluate security risks associated with the sharing of personal information; ensure there is a proper governance structure in place to support privacy including privacy leadership and a comprehensive contract; and ensure individuals have access to their personal information and information about its use.

6. Add a requirement in FIPPA that PIAs must be completed at the conceptual, design, and implementation phases of an electronic record project.

The comments made by the Honourable Dr. Margaret MacDiarmid's at first reading of *Bill 3, Freedom of Information and Protection of Privacy Amendment Act, 2011*[3] were as follows.

> *The* [FIPPA] *we have today came into force 19 years ago in 1992. These amendments modernize the act, aligning it with modern technology while ensuring that we do so in a way that maintains and enhances privacy. These amendments reflect the reality of how British Columbians interact with each other and with government today.*
>
> *We worked closely with the Information and Privacy Commissioner on these amendments. We have balanced new capabilities with the addition of strong new oversight powers for the commissioner.*

In her letter to Minister MacDiarmid, then Minister of Labour, Citizens' Services and Open Government, Commissioner Denham stated the following.[4]

> *In relation to privacy, the proposed amendments strike a workable balance between government's operational needs to share data for the purpose of integrated service delivery with appropriate oversight by the Information and Privacy Commissioner. I will work with government to develop a new information-sharing code of practice and new regulations for data linking, as well as other matters to be prescribed by regulation.*
>
> *The proposed mandatory requirement for privacy impact assessments and prior notice of integrated programs and data-linking initiatives are critical to ensure privacy risks are identified and properly addressed. Our intention would be to develop guidelines for public bodies on the types of information that my office would require in order to be able to review and comment on their privacy impact assessments.*

<u>BC's FIPPA Prior to the 2011 Amendments</u>

Section 26 of BC's FIPPA stated the following about the authority to collect personal information.

> *26 No personal information may be collected by or for a public body unless*
>
> > *(a) the collection of that information is expressly authorized under an Act,*
> >
> > *(b) that information is collected for the purposes of law enforcement, or*

---

[3] *Bill 3 – Freedom of Information and Protection of Privacy Amendment Act, 2011,* located at: http://www.leg.bc.ca/39th4th/1st_read/gov03-1.htm.

[4] Letter to the Honourable Dr. Margaret MacDiarmid from Commissioner Denham in respect of the FIPPA amendments, October 4, 2011, located at: https://www.oipc.bc.ca/public-comments/1139.

(c) that information relates directly to and is necessary for an operating program or activity of the public body.

Subsection 33.2 (d) of BC's FIPPA authorized a BC Public Body to disclose personal information referred to in section 33 inside Canada to:

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

Prior to the 2011 amendments, there was nothing in the *Freedom of Information and Protection of Privacy Regulation* (FIPPA Regulation) about requirements associated with a common or integrated program or activity. Schedule 1 of the FIPPA Regulation did not contain a definition for what a common or integrated program or activity was or definitions of data-linking, a data-linking initiative, or the provincial identity information services provider.

In Part 6 of the General Provisions, subsection 69 (1) of BC's FIPPA stated the following.

69 (1) In this section:

"information-sharing agreement" means an agreement that sets conditions on one or more of the following:

(a) the exchange of personal information between a public body and a person, a group of persons or an organization;

(b) the disclosure of personal information by a public body to a person, a group of persons or an organization;

(c) the collection of personal information by a public body from a person, a group of persons or an organization;

"personal information bank" means a collection of personal information that is organized or retrievable by the name of an individual or by an identifying number, symbol or other particular assigned to an individual;

"privacy impact assessment" means an assessment that is conducted to determine if a new enactment, system, project or program meets the requirements of Part 3 of this Act.

(2) The minister responsible for this Act must maintain and publish a personal information directory to provide information about records in the custody or under the control of ministries of the government of British Columbia and about the use of those records.

(3) The personal information directory must include a summary that meets the requirements of the minister responsible for this Act of the following information:

> *(a) the personal information banks that are in the custody or control of each ministry of the government of British Columbia;*
>
> *(b) the information-sharing agreements into which each ministry of the government of British Columbia has entered;*
>
> *(c) the privacy impact assessments that each ministry of the government of British Columbia has conducted;*
>
> *(d) any other information the minister responsible for this Act considers appropriate.*

(4) The head of a ministry must correct as soon as possible any errors or omissions in the portion of the personal information directory that relates to the ministry, and provide the corrected information to the minister responsible for this Act.

(5) The head of a ministry must conduct a privacy impact assessment and prepare an information-sharing agreement in accordance with the directions of the minister responsible for this Act.

(6) The head of a public body that is not a ministry must make available for inspection and copying by the public a directory that lists the public body's personal information banks and includes the following information with respect to each personal information bank:

> *(a) its title and location;*
>
> *(b) a description of the kind of personal information and the categories of individuals whose personal information is included;*
>
> *(c) the authority for collecting the personal information;*
>
> *(d) the purposes for which the personal information was obtained or compiled and the purposes for which it is used or disclosed;*
>
> *(e) the categories of persons who use the personal information or to whom it is disclosed;*
>
> *(f) information required under subsection (7).*

(7) The minister responsible for this Act may require one or more public bodies, or classes of public bodies, that are not ministries of the government of British Columbia

> *(a) to provide additional information for the purposes of subsection (6), and*

(b) to comply with one or more of the subsections in this section as if the public body were a ministry of the government of British Columbia.

(8) Not later than 60 days after making an order under section 33.1 (3) (orders allowing disclosure outside Canada), the minister responsible for this Act must publish a summary of the order.

Amendments to BC's FIPPA after November 2011[5]

The amendments to BC's FIPPA broadened the authority to collect personal information under section 26 to include five new circumstances in which a BC Public Body may collect personal information. These circumstances include collection with the consent of an individual in prescribed circumstances (subsection (d)), and collection if the information is personal identity information and it is collected by or from a provincial identity information services provider (subsection (h)). The following outlines amendments made to section 26 as well as additional amendments made in 2011.

Purposes for which personal information may be collected

26 A public body may collect personal information only if

(a) the collection of the information is expressly authorized under an Act,

(b) the information is collected for the purposes of law enforcement,

(c) the information relates directly to and is necessary for a program or activity of the public body,

(d) with respect to personal information collected for a prescribed purpose,

(i) the individual the information is about has consented in the prescribed manner to that collection, and

(ii) a reasonable person would consider that collection appropriate in the circumstances,

(e) the information is necessary for the purposes of planning or evaluating a program or activity of a public body,

(f) the information is necessary for the purpose of reducing the risk that an individual will be a victim of domestic violence, if domestic violence is reasonably likely to occur,

[5] *Ibid.* 3.

(g) the information is collected by observation at a presentation, ceremony, performance, sports meet or similar event

(i) at which the individual voluntarily appears, and

(ii) that is open to the public, or

(h) the information is personal identity information that is collected by

(i) a provincial identity information services provider and the collection of the information is necessary to enable the provincial identity information services provider to provide services under section 69.2, or

(ii) a public body from a provincial identity information services provider and the collection of the information is necessary to enable

(A) the public body to identify an individual for the purpose of providing a service to the individual, or

(B) the provincial identity information services provider to provide services under section 69.2.

The following was added to the FIPPA Regulation to address the consent requirements in subsection 26 (d) of BC's FIPPA.

Purposes for collection of personal information

9 For the purposes of section 26 (d) of the Act, personal information may be collected for one or more of the following purposes:

(a) to allow one or more

(i) public bodies, and

(ii) government institutions subject to the Privacy Act (Canada) specified by the individual to record or update

(iii) the individual's personal contact information, including the individual's address, phone number and e-mail address, and

(iv) the individual's name, if the individual has changed his or her name under the Name Act;

(b) if the person is acting for a deceased individual under section 5 of this regulation, to allow one or more

(i) public bodies, and

(ii) government institutions subject to the Privacy Act (Canada) specified by the person to receive notification of the death in order that benefits or services relating to the deceased may be provided or cancelled, as applicable.

Consent respecting personal information

11 (1) For the purposes of section 26 (d)…of the Act, consent must

(a) be in writing, and

(b) be done in a manner that specifies

(i) the personal information for which the individual is providing consent, and

(ii) the date on which the consent is effective and, if applicable, the date on which the consent expires.

(2) In addition to the requirements of subsection (1) of this section, for the purposes of

(a) section 26 (d) of the Act, consent must be done in a manner that specifies

(i) who may collect the personal information, and

(ii) the purpose of the collection of the personal information

Subsection 33.2 (d) of BC's FIPPA did not change. The term "common or integrated program or activity" was defined in Schedule 1 of BC's FIPPA as follows:

"common or integrated program or activity" means a program or activity that

(a) provides one or more services through
(i) a public body and one or more other public bodies or agencies working collaboratively, or
(ii) one public body working on behalf of one or more other public bodies or agencies, and

(b) is confirmed by regulation as being a common or integrated program or activity;

"Program or activity" was also defined in Schedule 1 of BC's FIPPA as:

"program or activity" includes, when used in relation to a public body, a common or integrated program or activity respecting which the public body provides one or more services;

The following was added to the FIPPA Regulation to address the requirement of section (b) of the definition of a "common or integrated program or activity" in Schedule 1 of BC's FIPPA.

Confirming a common or integrated program or activity

12 The written documentation that confirms that a program or activity is a common or integrated program or activity is a written agreement that

(a) is signed by the head of each public body and agency through which, or on whose behalf, as applicable, the services of the program or activity are provided, and

(b) includes the following:

(i) a description of the services provided by the program or activity;

(ii) a description of the types of personal information collected, used and disclosed in the course of providing the program or activity;

(iii) a description of the purposes, key objectives and expected benefits or outcomes of the program or activity;

(iv) a description of the respective roles and responsibilities of each public body and agency through which, or on whose behalf, the services are provided;

(v) the date on which the program or activity will start and, if applicable, the date on which the program or activity will end.

Division 3 of Part 3 was added to BC's FIPPA.

36.1 (1) A public body participating in a new or significantly revised data-linking initiative must comply with the regulations, if any, prescribed for the purposes of this subsection.

(2) If all the participants in a new or significantly revised data-linking initiative are a health care body, the ministry of the minister responsible for the administration of the Ministry of Health Act *or a health-related organization as prescribed, then subsection (1) does not apply to the participants.*

(3) For the purposes of subsections (1) and (2), a public body is participating in

(a) a new data-linking initiative if the data-linking initiative is implemented after the date this section comes into force, or

(b) a significantly revised data-linking initiative if the data-linking initiative is an existing data-linking initiative and a public body participating in that data-linking initiative expands it by doing one or more of the following:

(i) adding a public body or an agency that is not already a participant in the data-linking initiative;

(ii) adding a database that is not already a part of the data-linking initiative;

(iii) undertaking a purpose that is not already a purpose of the data-linking initiative;

(iv) using a type of technology that is not already a part of the data-linking initiative.

(4) Despite subsection (3) (a), a public body is not participating in a new data-linking initiative if, before the date this section comes into force, the public body has completed a written project plan respecting the data-linking initiative that states

(a) the objectives of the project,

(b) the costs and benefits of the project, and

(c) the risks associated with those costs and benefits.

In section 69 of BC's FIPPA, the definitions of information sharing agreement and privacy impact assessments were repealed and replaced with the following.

"information-sharing agreement" means an agreement between a public body and one or more of the following:

(a) another public body;

(b) a government institution subject to the Privacy Act *(Canada);*

(c) an organization subject to the Personal Information Protection Act *or the* Personal Information Protection and Electronic Documents Act *(Canada);*

(d) a public body, government institution or institution as defined in applicable provincial legislation having the same effect as this Act;

(e) a person or a group of persons;

(f) a prescribed entity,

that sets conditions on the collection, use or disclosure of personal information by the parties to the agreement;

"privacy impact assessment" means an assessment that is conducted by a public body to determine if a current or proposed enactment, system, project, program or activity meets or will meet the requirements of Part 3 of this Act.

Subsection 69 (5) of BC's FIPPA was repealed and replaced with the following.

69 (5) The head of a ministry must conduct a privacy impact assessment in accordance with the directions of the minister responsible for this Act.

(5.1) The head of a ministry, with respect to a proposed enactment, system, project, program or activity, must submit, during the development of the proposed enactment, system, project, program or activity, the privacy impact assessment to the minister responsible for this Act for the minister's review and comment.

(5.2) If the minister responsible for this Act receives a privacy impact assessment under subsection (5.1) respecting a common or integrated program or activity or a data-linking initiative, the minister must submit, during the development of the proposed enactment, system, project, program or activity, the privacy impact assessment to the commissioner for the commissioner's review and comment.

(5.3) The head of a public body that is not a ministry must conduct a privacy impact assessment in accordance with the directions of the minister responsible for this Act.

(5.4) The head of a public body that is not a ministry, with respect to a proposed system, project, program or activity, must submit, during the development of the proposed system, project, program or activity, the privacy impact assessment, if it addresses a common or integrated program or activity or a data-linking initiative, to the commissioner for the commissioner's review and comment.

(5.5) The head of a public body must notify the commissioner of a data-linking initiative or of a common or integrated program or activity at an early stage of developing the initiative, program or activity.

(5.6) If all the participants in a data-linking initiative are either a health care body, the ministry of the minister responsible for the administration of the Ministry of Health Act *or a health-related organization as prescribed, then*

> *(a) subsections (5.3), (5.4) and (5.5) do not apply with respect to a participant that is a health care body or a health-related organization as prescribed, and*
>
> *(b) subsections (5), (5.1) and (5.5) do not apply with respect to a participant that is the ministry of the minister responsible for the administration of the* Ministry of Health Act*.*

(5.7) The head of a ministry must prepare an information-sharing agreement in accordance with the directions of the minister responsible for this Act

Subsection 69 (9) of BC's FIPPA was added.

(9) The minister responsible for this Act, in consultation with the commissioner, must establish an information-sharing code of practice that makes recommendations respecting how personal information is to be collected, used and disclosed under this Act.

Section 69.2 of BC's FIPPA was added.

Provincial identity information services provider

69.2 (1) The minister responsible for this Act may designate a public body as a provincial identity nformation services provider.

(2) A provincial identity information services provider, by exercising its powers respecting the collection, use and disclosure of information, may provide the following services:

(a) identifying an individual;

(b) verifying the identity of an individual;

(c) updating personal identity information about an individual;

(d) issuing a physical or an electronic credential to an individual;

(e) managing the information associated with a physical or an electronic credential;

(f) any other service related to personal identity information that the minister responsible for this Act considers appropriate.

(3) The minister responsible for this Act may give directions to a provincial identity information services provider or a public body respecting

(a) the type and quantity of personal identity information required to identify, or verify the identity of, individuals seeking access to government services,

(b) the provision to individuals of physical and electronic credentials for use in accessing government services,

(c) the privacy and security of personal identity information that is collected, used or disclosed under this Act,

(d) the format in which personal identity information is collected, used or disclosed under this Act, and

(e) the circumstances in which particular types of personal identity information may or may not be collected, used or disclosed in relation to services provided under subsection (2).

(4) The minister, under subsection (3), may give different directions for different categories of personal identity information, personal identity information services and government services.

In addition to the definitions noted above, the following definitions were also added to Schedule 1 of BC's FIPPA.

"data linking" means the linking or combining of personal information in one database with personal information in one or more other databases if the purpose of the linking or combining is different from

(a) the purpose for which the information in each database was originally obtained or compiled, and

(b) every purpose that is consistent with each purpose referred to in paragraph (a);

"data-linking initiative" means a new or newly revised enactment, system, project, program or activity that has, as a component, data linking between

(a) two or more public bodies, or

(b) one or more public bodies and one or more agencies;

"provincial identity information services provider" means a provincial identity information services provider designated under section 69.2 (1)

AB'S FOIP ACT

In Commissioner Clayton's submissions on amendments to AB's FOIP Act in relation to the use of technology and information sharing by AB's Public Bodies, she recommended the following.[6]

- Proposed information sharing initiatives should be thoroughly reviewed and assessed for access and privacy implications before implementation.
- Resources should be dedicated to education, training and resource materials.
- Cross-sectoral information sharing initiatives undertaken by AB's Public Bodies should be registered with AB's Commissioner's office or a designated AB Government ministry.
- Legislative schemes authorizing information sharing without consent must ensure all participants are subject to AB's information and privacy laws.
- AB's Public Bodies conduct and submit PIAs to AB's Commissioner for proposed initiatives (including information sharing initiatives that involve data matching or are cross-sectoral), schemes or programs that meet certain criteria.

[6] Becoming a Leader in Access and Privacy, Submissions to the 2013 Government of Alberta FOIP Act Review, July 2013, Commissioner Jill Clayton, located at: http://www.oipc.ab.ca/Content_Files/Files/Publications/FOIP_Act_Review_2013_Becoming_A_Leader.pdf.

- Stakeholders participating in cross-sectoral information sharing initiatives should be required to record disclosures and legislation should ensure these records are accessible to individuals,
- AB's Public Bodies should be required to report breaches of privacy to AB's Commissioner.[7]

AB's FOIP Act has been under review since 2013. No amendments have been made since November 1, 2013.

Currently, the collection and use provisions in AB's FOIP Act are similar to those in the ATIPP Act, with AB's FOIP Act requirements regarding collection the same as the ATIPP Act section 29.

Following are previous amendments to AB's FOIP Act that are relevant to the use of technology and information sharing practices.

In 1999, AB's FOIP Act was amended to include subparagraph 38 (a) (ii) (g.1) which is now subsection 40 (1) in the current version.[8]

> *Disclosure of personal information*
>
> *40(1) A public body may disclose personal information only to an officer or employee of a public body or to a member of the Executive Council, if the disclosure is necessary for the delivery of a common or integrated program or service and for the performance of the duties of the officer or employee or member to whom the information is disclosed*

The amendments made to AB's FOIP Act also authorized the creation of a regulation to develop standards and procedures to be followed for data matching, data sharing or data linkage at paragraph 88 (a)(ii), now subsection 94 (1). No such regulation has been developed.

> *94(1) The Lieutenant Governor in Council may make regulations*
>
> *(k)respecting standards to be observed and procedures to be followed by a public body implementing a program for data matching, data sharing or data linkage;*

The Committee[9] charged with review of AB's FOIP Act in 1998, which led to the foregoing amendments, made the following comments about the amendments to subparagraph 38 (a) (ii) (g.1) and paragraph 88 (a) (ii).[10]

---

[7] *Ibid*. 6.

[8] *Bill 37, Freedom of Information and Protection of Privacy Amendment Act, 1999*, located at: http://www.assembly.ab.ca/ISYS/LADDAR_files/docs/bills/bill/legislature_24/session_3/19990216_bill-037.pdf.

[9] The Select Special Freedom of Information and Protection of Privacy Act Review Committee.

[10] Final Report of the Select Special Freedom of Information and Protection of Privacy Act Review Committee, March 1999, http://www.assembly.ab.ca/pro/FOIP/default.htm.

Section 38(1)(g) of the Act permits disclosure of personal information to officials within the same public body where a person has the need to know the information in order to perform his or her duties. Joint delivery of programs and services is becoming increasingly more important for efficiency in departments, agencies and local public bodies.

It was suggested that this provision be amended to enable public bodies to share information to administer joint programs.

Recognizing the need to restrict broad use of personal information for unrelated purposes, it was agreed that disclosure between public bodies should be permitted only for the administration of a common program, the Committee recommended:

> *That section 38(1)(g) of the Act should be amended to allow for the disclosure of personal information to an officer or employee of another public body where it is necessary to deliver a common program.*

Section 36 of the Act requires public bodies to ensure that reasonable security arrangements are maintained for personal information in their possession. These arrangements are currently outlined in policy.

It was generally agreed that legislation was the most appropriate place to set out protection principles, but at the same time, because of rapid changes in technology, it is often most practical to address technical matters, particularly in relation to data security, through the more flexible vehicle of regulation. Doing so by policy was not considered adequate. On this point, the Committee recommended:

That security and protection requirements related to computer data matching, data sharing and data linkage of personal information, which are now outlined in policy, should be specified in the FOIP Regulation at a minimum, and in the FOIP Act where possible.

Under AB's FOIP Act, AB's Public Bodies must publish a contact name responsible for administration of the FOIP Act (subsection 87 (2)) and a directory of personal information banks (section 87.1). AB's Public Bodies must also provide facilities to allow public inspection of documents used in decision-making processes.

Access to manuals

89(1) The head of every public body must provide facilities at

(a) the headquarters of the public body, and

(b) any offices of the public body that, in the opinion of the head, are reasonably practicable, where the public may inspect any manual, handbook or other guideline used in decision-making processes that affect the public by employees of the public body in administering or carrying out programs or activities of the public body.

(2) Any information in a record that the head of a public body would be authorized to refuse to give access to pursuant to this Act may be excluded from the manuals, handbooks or guidelines that may be inspected pursuant to subsection (1).

SK'S FOIP

In his recent Annual Report[11], Commissioner Kruzeniski made no recommendations specifically about amending SK's FOIP to address information sharing and the use of technology, but he did recommend the following.

- SK government institutions should be required to report a breach of privacy to the SK's Commissioner.
- SK government institutions should be required to prepare and submit to SK's Commissioner for his review and comment a PIA that describes how proposed administrative practices and information systems relating to the collection, use and disclosure of personal information may affect individuals' privacy.
- PIAs should be required to be submitted to SK's Commissioner prior to implementing any proposed new practice or system or any proposed change to existing practices or systems.

Similar recommendations were included in the recommendations made by BC's and AB's Commissioners related to information sharing and use of technology as a measure to improve privacy protection.

Following are sections of SK's FOIP and the *Freedom of Information and Protection of Privacy Regulations* (FOIP Regulations) that authorize or facilitate the use of technology and information sharing.

SK's FOIP authorizes a SK government institution to disclose information under paragraph 29 (2)(u) "as prescribed in the FOIP Regulations." The FOIP Regulations contain the following provision.[12]

16 For the purpose of clause 29 (2)(u) of the Act, personal information may be disclosed

(a) to another government institution[13] or a local authority for the purposes of:

[11] It's Time to Update, Office of the Saskatchewan Information and Privacy Commissioner's 2014-2015 Annual Report, Commissioner Ronald Kruzeniski, March 2015, located at: http://www.oipc.sk.ca/Annual_Reports/Annual_Report_2014-2015.pdf.

[12] The earliest version available online dates back to April 2004. This provision was contained in the Regulation then.

[13] Is similar to the meaning of public body in the ATIPP Act.

(i) determining the eligibility of an individual to participate in a program of, or receive a product or service from, the Government of Saskatchewan, a government institution or a local authority, in the course of processing an application made by or on behalf of the individual to whom the information relates;

(ii) verifying the eligibility of an individual who is or was participating in a program of, or receiving a product or service from, the Government of Saskatchewan, a government institution or a local authority;

(iii) verifying the accuracy of personal information held by the other government institution or the local authority; or

(iv) collecting a debt or assisting in the collection of a debt owing to Her Majesty in right of Saskatchewan, a government institution or a local authority;

(c) where disclosure may reasonably be expected to assist in the provision of services for the benefit of the individual to whom the information relates;

The collection provision in SK's FOIP is similar to subsection 29 (c) in the ATIPP Act.

MB'S FIPPA

When MB's FIPPA was reviewed in 2004, the Honourable Eric Robinson, former Minister of Culture, Heritage and Tourism for the Manitoba Government identified the following in the review consultation document about the need to modify the privacy provisions of MB's FIPPA to support technological innovation to improve service delivery. [14]

Research and everyday experience tells governments and other public bodies that citizens want, and increasingly expect to access government information and services easily and conveniently, preferably close to their community and at a time of their choosing.

Governments worldwide are responding to these expectations through electronic service delivery and integrated service offices.

Inevitably, changing the way services are delivered will change the way in which personal information is handled.

FIPPA generally does not allow government departments and agencies to share personal information with each other, except under certain specified conditions.

[14] Tell Us What You Think, A Review of The Freedom of Information and Protection of Privacy Act, January 2004, located at: http://www.gov.mb.ca/chc/fippa/pdfs/discussion.pdf.

Under an enhanced service delivery model, government bodies may need to share personal information in new ways to deliver services.

In "one-stop shops" offering a variety of interactive services, it may be necessary for staff, as well as citizens, to access personal data from several different sources. It may be necessary to draw on personal contact history from databases across the government or public body to make decisions about services such as eligibility for social assistance, issuing a particular license, reviewing payments or verifying facts.

Information technology makes it possible to bring together all kinds of personal information outside of the traditional office that gathered and kept files for its own limited uses.

Technology means that services and activities of government can be carried out faster and more efficiently.

A major challenge of all governments in the 21st century is finding a balance between protecting individual privacy and meeting wider social needs.

In the document, the Minister requested public input on the types of services citizens wanted delivered online or through a consolidated service unit, the benefits expected from this type of service delivery, and the safeguards citizens expect for these kinds of initiatives to adequately protect their personal information.

Former Ombudsman, Barry Tuckett, made a number of recommendations in respect of MB's FIPPA that he submitted to Minister Robinson. None were specific to information sharing and the use of technology.[15] He did, however, recommend the following.

- The use of PIAs to understand the potential impact of a proposed program, practices, services, or system on information privacy.
- That it be made clear in MB's FIPPA that information disclosed to a provider of information technology services is deemed to be under the control of a public body.
- Information security safeguards required to secure personal information should be similar to those found in SK's Personal Health Information Regulation: written policies and procedure, access restrictions, additional safeguards for electronic health information systems, authorized access for employees, orientation and training for employees, pledge of confidentiality for employees, and audit.

[15] By letter dated June 9, 2004, located at: https://www.ombudsman.mb.ca/uploads/files/news/65//fippa-review-2004.pdf.

Similar recommendations were included in the recommendations made by BC's and AB's Commissioners related to information sharing and use of technology as a measure improve privacy protection.

Following are the main amendments resulting from the review to facilitate information sharing and use of technology in MB's FIPPA.

Paragraph 44 (1)(f) was added.

44 (1) A public body may disclose personal information only

(f.1) to an officer or employee of a public body, for the purpose of delivering a common or integrated service, program or activity, if the information is necessary to deliver the service, program or activity and the officer or employee to whom the information is disclosed needs the information to carry out his or her responsibilities;

Several provisions in respect of an information manager were added.

Public body may provide information to an information manager

44.1(1) A public body may provide personal information to an information manager for the purpose of processing, storing or destroying it or providing the public body with information management or information technology services.

Agreement required

44.1(3) A public body that wishes to provide personal information to an information manager under this section must enter into a written agreement with the information manager that provides for the protection of the personal information against such risks as unauthorized access, use, disclosure, destruction or alteration, in accordance with the regulations.

Information manager shall comply with Act

44.1(4) An information manager shall comply with

(a) the same requirements concerning the protection of personal information that the public body is required to comply with under this Act; and

(b) the duties imposed on the information manager under the agreement entered into under subsection (3).

Information deemed to be maintained by the public body

44.1(5) Personal information that has been provided to an information manager under an agreement described in subsection (3) is deemed to be in the custody and control of the public body for the purposes of this Act.

Part 4.1 was added authorizing the Ombudsman[16] to refer a matter to an arbitrator if a MB Public Body refuses to implement a recommendation or take any action respecting a recommendation, including implementing or failing to respond to the Ombudsman's recommendations.

There were no amendments to MB's FIPPA's purpose of collection provision which is similar to the collection provision in the ATIPP Act.

The MB's Ombudsman's Office is unaware how or if these provisions are being used as authority to share information for integrated services.

ON'S FOIPPA

On second reading of *Bill 152, Ministry of Government Services Consumer Protection and Service Modernization Act*, 2006, the Honourable Gerry Phillips, former Minister of Government Services stated the following.[17]

> *We have an organization within my ministry called Service Ontario. Its role is ultimately to be the one-stop shop for the public when they're looking for information or services from government. In order for that to happen, we need the legal authority to make sure they are able to offer a broad range of government information and services.*

The amendments to ON's FOIPPA contained in the Bill, which took effect on April 1, 2007, resulted in the addition of the following section.

> *Service provider organizations*
>
> *65.1 (1) This section applies with respect to a service provider organization as defined in section 17.1 of the Ministry of Government Services Act.*
>
> *Definitions*
>
> *(2) In this section,*
>
> *"customer service information" means, in relation to a service,*

[16] The Manitoba Ombudsman is responsible for oversight of FIPPA.

[17] *Bill 152, Ministry of Government Services Consumer Protection and Service Modernization Act*, 2006, located at: http://www.ontla.on.ca/web/bills/bills_detail.do?locale=en&BillID=478&isCurrent=false&detailPage=bills_detail_the_bill.

(a) the name, address and telephone number or other contact information of the individual to whom the service is to be provided and, if applicable, the person acting on behalf of that individual,

(b) the transaction or receipt number provided by the service provider organization in relation to the request for the service,

(c) information relating to the payment of any fee, and

(d) such other information as may be prescribed;

"designated service" means a service designated by regulations made under subsection 17.1 (3) of the Ministry of Government Services Act as a service that the service provider organization may provide on behalf of the Government or a public body;

"Government" means the Government as defined in the Ministry of Government Services Act;

"public body" means a public body as defined in section 17.1 of the Ministry of Government Services Act.

Authorization to collect personal information(3) A service provider organization is authorized to collect personal information for the purposes of providing a designated service.

Collection of customer service information

(4) Without limiting the generality of subsection (3), a service provider organization is authorized to collect customer service information, with the consent of the individual to whom the information relates, for the purposes of providing a designated service.

Conveying information to the Government, etc.

(5) If required by the regulations, a service provider organization that collects personal information on behalf of the Government or a public body in the course of providing a designated service shall convey the personal information to that Government or public body in accordance with the regulations.

Limitation after information conveyed

(6) After the service provider organization has conveyed personal information under subsection

(5), the service provider organization shall not use or further disclose the personal information except as allowed by the regulations.

Collection of personal information under arrangements

(7) A person who provides services on behalf of a service provider organization pursuant to an arrangement under subsection 17.1 (7) of the Ministry of Government Services Act may not collect personal information in connection with providing those services unless the service provider organization and the person have entered into an agreement that governs the collection, use and disclosure of such personal information and the agreement meets the prescribed requirements, if any.

Audits by Commissioner

(8) The Commissioner may audit a service provider organization to check that there has been no unauthorized access to or modification of personal information in the custody of the organization and the organization shall co-operate with and assist the Commissioner in the conduct of the audit.

ON's FOIPPA authorizes the development of regulations in respect of section 65.1 and requires the Minister to do public consultation prior to developing and implementing the regulations.[18] To date, no regulations have been developed in respect of section 65.1.

Subsection 17.1 of ON's *Ministry of Government Services Act* states the following:

(1) The Lieutenant Governor in Council may, by regulation, designate a ministry of the Government of Ontario, part of such a ministry or a person or entity as an organization to provide services to members of the public on behalf of the Government or a public body. 2006, c. 34, Sched. F, s. 2.

Note: On a day to be named by proclamation of the Lieutenant Governor, subsection (1) is repealed and the following substituted:

Service provider organizations

Designation

(1) The Lieutenant Governor in Council may, by regulation, designate a ministry of the Government of Ontario or part of such a ministry as an organization to provide services to members of the public on behalf of the Government or a public body. (2).

[Shading in original]

Definitions

(2) In this section,

"public body" means,

[18] See subsections 65.1 (9) and 65.2.

(a) a related government,

(b) the corporation of any municipality in Ontario,

(c) a local board, as defined in the Municipal Affairs Act, and any authority, board, commission, corporation, office or organization of persons some or all of whose members, directors or officers are appointed or chosen by or under the authority of the council of the corporation of a municipality in Ontario,

(d) such other persons and entities as may be prescribed;

"service" means anything that may be done by the Government or public body in interacting with members of the public.

Designation of services to be provided

(3) If the Lieutenant Governor in Council designates a service provider organization under subsection (1), the Lieutenant Governor in Council shall make regulations designating services,

(a) that the service provider organization may provide on behalf of the Government; or

(b) that the service provider organization may provide on behalf of a public body if the service provider organization is so authorized by that public body or by a person or entity who, under any other law, may give such an authorization.

Authorization to exercise powers under statute, etc.

(4) To facilitate the provision of services by the service provider organization on behalf of the Government or a public body, the Lieutenant Governor in Council may make regulations,

(a) authorizing the service provider organization to exercise powers or perform functions or duties under an Ontario statute or regulation;

(b) providing for a reference in an Ontario statute or regulation to the person who would otherwise exercise a power or perform a function or duty referred to in clause (a) to be read, to the extent specified in the regulations, as though the reference was to the service provider organization.

Limitation

(5) Regulations under subsection (4) may not provide for the service provider organization to make regulations or conduct any review or appeal..

Authorization in addition to other powers to delegate, etc.

(6) For greater certainty, the power to make regulations authorizing the service provider organization to exercise powers or perform functions or duties under an Ontario statute or regulation is in addition to, and does not derogate from, any authority, under the statute, regulation or any other law, to delegate or assign such a power, function or duty.

Arrangements with others

(7) A service provider organization may arrange with another person to provide services on behalf of the service provider organization or exercise powers or perform functions or duties that the service provider organization is authorized to exercise or perform.

There is also authority for the creation of regulations and standards related to the provision of services.[19]

In ON's *Ministry of Government Services Act, Ontario Regulation 475/07*, Service Ontario is designated as a service provider organization. Several services are designated including the following:

- Government of Ontario: administrative services,
- Ministry of Community Safety and Correctional Services: private investigators and security guard licences, and administrative services,
- Ministry of Health and Long-Term Care: health cards and organ donor registration, and administrative services,
- Minister of Natural Resources: fishing licences, hunting licences, trapping licences, processing, buying and selling wildlife, crown land and camping permits, and administrative services,
- Ministry of Revenue: administrative services,
- Ministry of Transportation: *Highway Traffic Act* licences, permits and plates, *Motorized Snow Vehicles Act* licences and permits, *Off-Road Vehicles Act* permits and plates, photo cards, Ministry records, and administrative services, and
- some municipality and Federal Government related services.

The Bill did not result in amendments to the collection and use provisions of ON's FOIPPA which are similar to those in the ATIPP Act.[20]

[19] See subsection 17.1 (8) and 17.2 of the *Ministry of Government Services Act.*

[20] Subsection 41 (d), the use provision of FOIPPA, was added in 2005 which authorizes an educational institution to use personal information in alumni records for fundraising.

NB'S RTIPPA

In his submission on *Bill 82, the proposed Access to Information and Protection of Information Act* which preceded *Bill 89, the Right to Information and Protection of Privacy Act*, former Ombudsman Richard, in reference to the growth in use of technology, recommended the following be added to the Bill to strengthen privacy protection.

- NB's Public Bodies should be required to register and demonstrate approved usage and storage safety practices for data banks.
- NB's Public Bodies should be required to register with NB's Commissioner[21] their personal information data banks and the type of information collected.
- NB's Public Bodies should be required to report breaches of personal information to NB's Commissioner.
- Regulations should be developed to facilitate online access to information, restrict data-mining, regulate data-sharing practices, and establish a range of privacy invasive technologies or surveillance technologies that would be subject to approval or review by NB's Commissioner prior to adoption or development "eg use of biometric data, video-surveillance cameras by schools or other public bodies."

Bill 89, *Right to Information and Protection of Privacy Act*, passed on May 29, 2009

Following are provisions in NB's RTIPPA relevant to the use of technology and the sharing of information.

Paragraph 46 (1)(c.1) authorizes NB's Public Bodies to disclose information for a common or integrated program or activity.

> *46(1) A public body may disclose personal information only*
>
> > *(c.1) to an officer or employee of another public body or a custodian who is a health care provider, as those terms are defined in the Personal Health Information Privacy and Access Act, if the information is necessary for the delivery of an integrated service, program or activity and for the performance of the duties, respecting the integrated service, program or activity, of the officer or employee or the custodian who is a health care provider to whom the information is disclosed.*

Sections 47, 77 and the *General Regulation, NB Reg 2010-111* establish a Privacy Assessment Review Committee (PAR Committee) to, *inter-alia*, review proposals by NB's Public Bodies for data linking or

[21] The Information and Privacy Commissioner for New Brunswick was established as a separate office from the Ombudsman's Office in Bill 89.

matching from different data bases and disclosure of a volume or bulk of data. Section 47 also establishes criteria that NB's Public Bodies must follow in relation to the PAR Committee.

Assessment required for other uses and disclosures

47(1) This section applies only to uses and disclosures not otherwise authorized under this Division.

47(2) A public body may only use or disclose personal information with the approval of the head of the public body if the public body

(a) proposes to use or disclose personal information in order to link information databases or match personal information in one information database with information in another,

(b) receives a request for disclosure of personal information for the purposes of legitimate research in the interest of science, learning or public policy, or

(c) receives a request for disclosure on a volume or bulk basis of personal information in a public registry or another collection of personal information.

47(3) If a proposal or request is made under subsection (2) by or to a department or a government body, the head shall refer it to the review committee for its advice.

47(4) If a proposal or request is made under subsection (2) by or to a local public body, the head may refer it to the review committee for its advice.

47(5) The review committee shall assess a proposal or request referred to it under this section and provide advice to the head of the public body about the matters referred to in subsection (6).

47(6) The head of the public body may approve the proposal or request made under subsection (2) only if

(a) any advice from the review committee under subsection (3) has been received and considered,

(b) the head is satisfied that

(i) the purpose of the proposal or request cannot reasonably be accomplished unless the personal information is provided in a form that identifies individuals,

(ii) it is unreasonable or impractical to obtain consent from the individuals the personal information is about, and

(iii) the use or disclosure is not likely to harm the individuals the personal information is about and the benefits to be derived from the use or disclosure are clearly in the public interest,

(c) the head has approved conditions relating to

(i) the use of the personal information,

(ii) the protection of the personal information, including security and confidentiality,

(iii) the removal or destruction of individual identifiers, if appropriate, at the earliest reasonable time,

(iv) any subsequent use or disclosure of the personal information in a form that identifies individuals without the express written authorization of the public body, and

(d) the recipient of the personal information has entered into a written agreement to comply with the approved conditions.

Privacy Assessment Review Committee

77 The Minister shall establish, in accordance with the regulations, a Privacy Assessment Review Committee for the purposes of section 47.

"review committee" means the Privacy Assessment Review Committee established by the Minister under section 77.

General Regulation, NB Reg2010-111

Privacy Assessment Review Committee

8(1) The review committee established under section 77 of the Act shall include a minimum of 5 members appointed by the Minister.

8(2) The Minister shall designate a chair of the review committee from among the members of the review committee.

There is no information available regarding the use or effectiveness of the PAR Committee.

The collection and use provisions in NB's RTIPPA are similar to those in the ATIPP Act.

The RTIPPA is currently under review. The discussion paper prepared for the review highlights[22] the provision that authorizes disclosure of information for integrated services, programs or activities and states the following about this provision.

> *One of the primary purposes of RTIPPA is to control how public bodies may collect, use and disclose personal information. These limitations are intended to protect personal privacy, not to impede public bodies from co-operating to deliver integrated programs or services.*
>
> *For this reason, RTIPPA was amended in 2013 to allow for the sharing of information in the context of an "authorized integrated service, program or activity" that provides support with respect to the mental, physical or social well-being of an individual.*

On the topic of "emerging trends," the discussion paper highlights the following.

> *Information technology has been making rapid advances in recent years. These changes have enabled faster and easier information sharing between individuals, between individuals and public bodies, and among public bodies, often to the benefit of the public.*
>
> *However, these innovations create challenges to protecting privacy. Although emerging technological tools and trends can be beneficial, some of the most popular pose privacy implications:*
>
> - *Data storage and the use of cloud computing raise security and therefore privacy concerns for public bodies.*
> - *Public bodies are increasingly accessing personal information made available through social media. The public may not always know that the information they post is being used in this way.*
> - *Individuals and businesses who enjoy the convenience of online private sector services are expecting the same level of service from their government.*
>
> *These trends are unlikely to slow down in the future. Public bodies that adopt these tools – and the public whom they serve – will continue to face challenges associated with the security and protection of the information posed by emerging technologies.*

The questions posed to the public in the discussion paper as it relates to the privacy provisions of the RTIPPA follow.

---

[22] Review of the Right to Information and Protection of Privacy Act Discussion Paper, Government Services, January 21, 2015 (Paper), located at: http://www2.gnb.ca/content/dam/gnb/Corporate/pdf/RTIPPA/RTIPPA_DiscussionPaper.pdf.

Are you satisfied that the personal information public bodies collect is being managed in such a way that individuals' privacy is protected?

Should government departments be allowed to share personal information if doing so would improve government programs and services?[23]

NS'S FOIPOP

The provisions contained in NS's FOIPOP Act are similar to those in the ATIPP Act. There are no provisions that would allow a NS Public Body to collect, use or disclose personal information for a common or integrated program or activity or for the purposes of centralized service delivery, such as identity services.

PEI'S FOIPP ACT

Bill No. 32, An Act to Amend the Freedom of Information and Protection of Privacy Act (No.2) included the amendments referred to below. The amendments were made to PEI's FOIPP Act following amendments to AB's FOIP Act on which PEI's FOIPP Act was originally modeled.

In the commentary[24] available online in respect of the amendments, no specific comments were made in relation to the privacy provisions of PEI's FOIPP Act.

Subsection 37 (g.1) of PEI's FOIPP Act authorizes PEI's Public Bodies to disclose personal information for a common or integrated program or activity.

37 (1) A public body may disclose personal information only

(g.1) to an officer or employee of a public body or to a member of the Executive Council, if the disclosure is necessary for the delivery of a common or integrated program or service and for the performance of the duties of the officer or employee or member to whom the information is disclosed;

Paragraphs 77 (1)(j) and (k) of PEI's FOIPP Act authorize the making of regulations to establish technical standards for information security and for data matching, data sharing and data linkage.

---

[23] The consultation process is closed. The website indicates a report will be tabled in respect of the review by August 31, 2015, located at: http://www2.gnb.ca/content/gnb/en/corporate/public_consultations/AccessAndPrivacyLegislativeReview.html.

[24] Including in Hansard debates and those provided by the Information and Privacy Commissioner. The debates in the House focused primarily on the access to information provisions.

77 (1) The Lieutenant Governor in Council may make regulations

(j) respecting technical standards and safeguards to be observed for the security and protection of personal information;

(k) respecting standards to be observed and procedures to be followed by a public body implementing a program for data matching, data sharing or data linkage;

No regulations exist in respect of these paragraphs.

The collection and use provisions of PEI's FOIPP Act are similar to those in the ATIPP Act.

NWT'S ATIPP ACT

The provisions contained in NWT's ATIPP Act are somewhat similar to those in the ATIPP Act. There are no provisions that would allow a public body to collect, use or disclose personal information for a common or integrated program or activity or for the purposes of centralized service delivery, such as identity services.

NU'S ATIPP ACT

NU's ATIPP Act has many of the same provisions as NWT's ATIPP Act including the collection, use and disclosure provisions. NU's ATIPP Act, however, has provisions that require a public body to report a breach of privacy to the Commissioner.

The following provisions, along with the ability of NU's Commissioner to conduct reviews of complaints about the inappropriate collection, use, or disclosure of personal information, were added following a review of NU's ATIPP Act and the Government of Nunavut's commitment to bring up the standard for protection of personal privacy to "the national standard."[25]

DIVISION E - DATA BREACH NOTIFICATION

Definition

[25] Report on the Review of the 2010-2011 Annual Report of the Information and Privacy Commissioner of Nunavut, Standing Committee on Oversight of Government Operations and Public Accounts, Third Session of the Third Legislative Assembly of Nunavut, March 2012, p.9, locate at: http://www.assembly.nu.ca/sites/default/files/OGOPA%20Report%20on%20the%20Review%20of%20the%202010-2011%20Annual%20Report%20of%20the%20Information%20and%20Privacy%20Commissioner%20of%20Nunavut%20-%20March%202012%20-%20English.pdf .

49.7 In this Division,

"harm" includes bodily harm, humiliation, damage to reputation, damage to a relationship, loss of an employment, business or professional opportunity, a negative effect on the credit record, damage to or loss of property, financial loss and identity theft. S.Nu. 2012, c.13,s.5.

Breach of Privacy

49.8 For the purposes of this Division, a breach of privacy occurs with respect to personal information if

> *(a) the information is accessed and the access is not authorized under this Act;*
>
> *(b) the information is disclosed and the disclosure is not authorized under this Act; or*
>
> *(c) the information is lost and the loss may result in the information being accessed or disclosed without authority under this Act. S.Nu. 2012, c.13,s.5.*

Public body to report to Information and Privacy Commissioner

49.9 (1) A public body that knows or has reason to believe that a breach of privacy has occurred with respect to personal information under its control shall report the breach of privacy to the Information and Privacy Commissioner in accordance with this section if the breach is material.

Material breach of privacy – factors

(2) The factors that are relevant in determining whether a breach of privacy with respect to personal information under the control of a public body is material include

> *(a) the sensitivity of the personal information;*
>
> *(b) the number of individuals whose personal information is involved;*
>
> *(c) the likelihood of harm to the individuals whose personal information is involved; and*
>
> *(d) an assessment by the public body whether the cause of the breach is a systemic problem.*

Time of report

(3) The report required by subsection (1) must be made as soon as reasonably possible after the public body knows or has reason to believe that the breach of privacy occurred and determines that the breach is material.

Content of report

(4) The report required by subsection (1) must describe the steps taken by the public body to comply with sections 49.10 and 49.11 and must contain such other information as may be prescribed. S.Nu. 2012, c.13,s.5.

Public body to notify individual

49.10. (1) A public body that knows or has reason to believe that a breach of privacy has occurred with respect to an individual's personal information under the public body's control shall notify the individual of the breach of privacy in accordance with this section if it is reasonable in the circumstances to believe that the breach of privacy creates a real risk of significant harm to the individual.

Real risk of significant harm – factors

(2) The factors that are relevant to determining whether a breach of privacy with respect to an individual's personal information creates a real risk of significant harm to the individual include

(a) the sensitivity of the personal information; and

(b) the probability that the personal information has been, is being or will be misused.

Time of notice

(3) The notice required by subsection (1) must be given as soon as reasonably possible after the public body knows or has reason to believe that the breach of privacy occurred and determines that the breach of privacy creates a real risk of significant harm to the individual.

Content of notice

(4) The notice required by subsection (1) must contain

(a) sufficient information to allow the individual to

(i) understand the significance to him or her of the breach of privacy, and

(ii) take steps, if any are possible, to reduce the risk of, or mitigate, any harm to him or her that could result from the breach of privacy;

(b) information describing what steps the public body has taken to reduce the risk of, or mitigate, any harm to the individual that could result from the breach of privacy; and

(c) such other information as may be prescribed. S.Nu. 2012, c.13,s.5.

Public body to notify others

49.11 A public body that notifies an individual of a breach of privacy under section 49.10 shall, at the same time, also notify a government institution, a part of a government institution or another public body of the breach of privacy if

> *(a) the government institution, part of a government institution or other public body may be able to reduce the risk of, or mitigate, any harm to the individual that could result from the breach of privacy; or*
>
> *(b) a prescribed condition is satisfied. S.Nu. 2012, c.13,s.5.*

Recommendation from Information and Privacy Commissioner to public body

49.12 If the Information and Privacy Commissioner receives a report under section 49.9 about a breach of privacy with respect to personal information under the control of a public body and determines that the breach of privacy creates a real risk of significant harm to one or more individuals to whom the information relates, the Information and Privacy Commission may recommend the public body to

> *(a) take steps specified by the Information and Privacy Commission relating to notifying those individuals about the breach of privacy, if the Information and Privacy Commissioner is of the opinion that the steps taken by the public body to comply with section 49.10 were not sufficient;*
>
> *(b) take steps specified by the Information and Privacy Commissioner to limit the consequences of the breach of privacy; and*
>
> *(c) take steps specified by the Information and Privacy Commissioner to prevent the occurrence of further breaches of privacy with respect to personal information under the public body's control, including, without limitation, implementing or increasing security safeguards within the public body. S.Nu. 2012, c.13,s.5.*

49.13 Within 30 days after receiving a recommendation under section 49.12, the head of the public body concerned shall

> *(a) make a decision to follow the recommendation of the Information and Privacy Commissioner or make any other decision the head considers appropriate; and*
>
> *(b) give written notice of the decision to the Information and Privacy Commissioner and any individual notified under section 49.10. S.Nu. 2012, c.13,s.5.*

Disclosure by Information and Privacy Commissioner

49.14 If the Information and Privacy Commissioner receives a report under section 49.9 about a breach of privacy with respect to personal information under the control of a public body and determines that the breach of privacy creates a real risk of significant harm to one or more

individuals to whom the information relates, the Information and Privacy Commissioner may, despite section 56,

> *(a) disclose the breach of privacy to the individuals in the manner that the Information and Privacy Commissioner considers appropriate, if the Information and Privacy Commissioner has given the public body a recommendation under clause 49.12(a) and the public body has not taken the steps specified in the recommendation within the times specified in the recommendation; and*
>
> *(b) disclose the breach of privacy to the public in the manner that the Information and Privacy Commissioner considers appropriate, if the Information and Privacy Commissioner is of the opinion that the disclosure is in the public interest. S.Nu. 2012, c.13,s.5.*

NL'S ATIPPA

NL's ATIPPA was amended in 2015 and those amendments have been brought into force. The recommendations made in respect of information sharing and the use of technology are set out below.

In NL's ATIPPA Review Report, the following was stated about the need to include mandatory breach reporting in the ATIPPA.

> *Data breaches did not appear to be a major concern of participants in the review exercise. Yet they are taking place.*
>
> *The apparent serenity about personal information challenges during the Committee's hearings and in written submissions may stem from the relatively little attention they received in the Act before 2012, which meant that fewer actions could be taken by the OIPC.*
>
> *Few references to data security issues exist in the ATIPPA as it is presently worded; the only specific mention is found in the following section:*
>
> > *The head of a public body shall protect personal information by making reasonable security arrangements against such risks as unauthorized access, collection, use, disclosure or disposal.*[26]
>
> *This reference in the Act to data breaches is no longer adequate, since public bodies other than those in the health sphere hold information of great interest to ill-motivated persons inside and*

[26] This is exactly the same wording as appears in section 33 in the ATIPP Act.

[27] See http://parcnl.ca/documents/full_report.pdf.

outside the public service. It is time for a serious examination of how the present legislation and its application deal with inevitable breaches in security of personal information.

The need for more effective protection of personal information is recognized internationally. The Privacy Commissioner of Canada pointed out that in the major Review of the Privacy Guidelines in 2013, the Organization for Economic Co-operation and Development (OECD) adopted new provisions recommending that member countries, which includes Canada, implement mandatory breach notification schemes.

Since relatively few data breaches from public bodies are documented, the optimal requirement would be to report all breaches to the Commissioner, who could recommend any necessary follow up, notification of the affected parties if that has not already been done, preventative measures for the future, and so on.

Data breach reporting better informs and protects individuals who may be the victims. It also sensitizes the public body and its personnel to the importance of data security at all times. Now that information held by public bodies is under increasing pressure from data predators, a workable notification scheme for data breaches is essential. The Commissioner addressed the value of reporting breaches:

> *While some public bodies have voluntarily reported significant breaches to this Office, such reporting is not required by law, and it tells us nothing about the state of overall privacy compliance. We are unable to spot trends or systemic issues, and therefore are unable to recommend steps to help prevent further breaches in the future*

The recommendation following these comments was as follows:

The Act be amended to require a public body to:

> *(a) report all privacy breaches to the Commissioner; and*
>
> *(b) notify affected individuals when there is a risk of significant harm created by a privacy breach.*

The following comments were made in respect of subsection 39 (1)(u), as it was prior to the 2015 amendments.

The OIPC noted that Bill 29 introduced increased data-sharing possibilities in section 39:

> *39 (1) A public body may disclose personal information only…*
>
> > *(u) to an officer or employee of a public body or to a minister, where the information is necessary for the delivery of a common or integrated program or service and for the performance of the duties of the officer or employee or minister to whom the information is disclosed.*

This means that new programs could be created, using information collected for another program and for another purpose, without an assessment as to the impact this would have on personal privacy.

NL's ATIPPA Review Report noted that, following a privacy breach investigation, NL's Commissioner recommended that NL's Public Bodies that are sharing personal information as part of a common or integrated program or activity or data linking initiative should complete PIAs and submit them to the Commissioner for review and comment. It was also noted that the department in the Government of NL responsible for the ATIPPA had created a policy requiring NL's Public Bodies to complete and submit PIAs for review and comment to the department. The following was stated in the Report in respect of the recommendation and the department's PIA policy:

Public bodies in Newfoundland and Labrador are gaining experience in preventative privacy exercises. A PIA is increasingly becoming a standard procedure before new ways are devised to collect, share, or disclose personal information. It is important that it be mandated here as well.

The Federal Government and the Office of the Privacy Commissioner of Canada have also placed increasing importance on privacy impact assessments to mitigate the effects of ever-wider information sharing, often undertaken for reasons relating to public safety and national security.

In his submission the Privacy Commissioner of Canada stressed that "privacy impact assessments are a valuable tool in fostering a greater institutional privacy culture and in consolidating internal accountability frameworks.

Also mentioned were BC's FIPPA requirements for PIAs as indicated above.

In recognition of the importance of using PIAs as a means to proactively protect privacy, in was concluded in NL's ATIPPA Review Report that:

…prevention is the optimal way of protecting personal information, and it can be achieved by clearly spelling out in the ATIPPA the following statutory obligations.

The first requirement is for departments to carry out privacy impact assessments where personal information is involved in the development of new government programs and services and to submit them to the minister responsible for the ATIPPA for review and comment.

Second, PIAs would also be forwarded to the Commissioner for his review and comment if they pertain to departments that address a common or integrated program or service for which disclosure of personal information may be permitted under section 39(1)(u).

The following amendments made to NL's ATIPPA in section 64 resulting from this recommendation expand on the requirement to secure personal information previously contained in NL's ATIPPA,[27] and,

[27] Section 36 of the version of ATIPPA in force between December 10, 2013 and May 31, 2015, located at: http://www.canlii.org/en/nl/laws/stat/snl-2002-c-a-1.1/latest/snl-2002-c-a-1.1.html

include a requirement that NL's Public Bodies notify individuals and the Commissioner about a privacy breach.

Protection of personal information

64 (1) The head of a public body shall take steps that are reasonable in the circumstances to ensure that

(a) personal information in its custody or control is protected against theft, loss and unauthorized collection, access, use or disclosure;

(b) records containing personal information in its custody or control are protected against unauthorized copying or modification; and

(c) records containing personal information in its custody or control are retained, transferred and disposed of in a secure manner.

(2) For the purpose of paragraph (1)(c), "disposed of in a secure manner" in relation to the disposition of a record of personal information does not include the destruction of a record unless the record is destroyed in such a manner that the reconstruction of the record is not reasonably foreseeable in the circumstances.

(3) Except as otherwise provided in subsections (6) and (7), the head of a public body that has custody or control of personal information shall notify the individual who is the subject of the information at the first reasonable opportunity where the information is

(a) stolen;

(b) lost;

(c) disposed of, except as permitted by law; or

(d) disclosed to or accessed by an unauthorized person.

(4) Where the head of a public body reasonably believes that there has been a breach involving the unauthorized collection, use or disclosure of personal information, the head shall inform the commissioner of the breach.

(5) Notwithstanding a circumstance where, under subsection (7), notification of an individual by the head of a public body is not required, the commissioner may recommend that the head of the public body, at the first reasonable opportunity, notify the individual who is the subject of the information.

(6) Where a public body has received personal information from another public body for the purpose of research, the researcher may not notify an individual who is the subject of the information that the information has been stolen, lost, disposed of in an unauthorized manner or disclosed to or accessed by an unauthorized person unless the public body that provided the information to the researcher first obtains that individual's consent to contact by the researcher and informs the researcher that the individual has given consent.

(7) Subsection (3) does not apply where the head of the public body reasonably believes that the theft, loss, unauthorized disposition, or improper disclosure or access of personal information does not create a risk of significant harm to the individual who is the subject of the information.

(8) For the purpose of this section, "significant harm" includes bodily harm, humiliation, damage to reputation or relationships, loss of employment, business or professional opportunities, financial loss, identity theft, negative effects on the credit record and damage to or loss of property.

(9) The factors that are relevant to determining under subsection (7) whether a breach creates a risk of significant harm to an individual include

(a) the sensitivity of the personal information; and

(b) the probability that the personal information has been, is being, or will be misused

Section 68 of NL's ATIPPA authorizes a NL Public Body to disclose personal information as part of a common or integrated program or activity. This provision was added in the amendments to NL's ATIPPA which took effect on June 30, 2012.

68 (1) A public body may disclose personal information only

(u) to an officer or employee of a public body or to a minister, where the information is necessary for the delivery of a common or integrated program or service and for the performance of the duties of the officer or employee or minister to whom the information is disclosed; or

The 2015 amendments to NL's ATIPPA included a requirement that NL's Public Bodies submit a PIA for any common or integrated program or service involving the collection, use and disclosure of personal information to the Minister and the Commissioner.

Privacy impact assessment

72 (1) A minister shall, during the development of a program or service by a department or branch of the executive government of the province, submit to the minister responsible for this Act

(a) a privacy impact assessment for that minister's review and comment; or

(b) the results of a preliminary assessment showing that a privacy impact assessment of the program or service is not required.

(2) A minister shall conduct a preliminary assessment and, where required, a privacy impact assessment in accordance with the directions of the minister responsible for this Act.

(3) A minister shall notify the commissioner of a common or integrated program or service at an early stage of developing the program or service.

(4) Where the minister responsible for this Act receives a privacy impact assessment respecting a common or integrated program or service for which disclosure of personal information may be permitted under paragraph 68 (1)(u), the minister shall, during the development of the program or service, submit the privacy impact assessment to the commissioner for the commissioner's review and comment.

The following amendments also pertain to the use of technology and information sharing.

Section 111 of NL's ATIPPA, requires NL's Commissioner to create a standard template for the publication of information, and the head of a NL Public Body is required to adapt the template for identifying and locating records, including personal information banks, in the Public Body.

The Minister responsible for NL's ATIPPA is required to consult with NL's Commissioner on any proposed Bills before the Bill is introduced in the House and to issue a Report addressing a number of items including any systemic and other issues raised by NL's Commissioner in his annual report.

Report of minister responsible

113. The minister responsible for this Act shall report annually to the House of Assembly on the administration of this Act and shall include information about

(a) the number of requests for access and whether they were granted or denied;

(b) the specific provisions of this Act used to refuse access;

(c) the number of requests for correction of personal information;

(d) the costs charged for access to records; and

(e) systemic and other issues raised by the commissioner in the annual reports of the commissioner

The collection and use[28] provisions of NL's ATIPPA are similar to those in the ATIPP Act.

[28] Except that in the ATIPPA, there is some additional uses authorized for post-secondary educational bodies. See section 67.