Office of the
Saskatchewan Information
and Privacy Commissioner

IT'S TIME TO UPDATE

Proposals for Amendments to

The Freedom of Information and Protection of Privacy Act

and

The Local Authority Freedom of Information and Protection of Privacy Act

Ronald J. Kruzeniski, Q.C.

March 2015

TABLE OF CONTENTS

INTRODUCTION

The Freedom of Information and Protection of Privacy Act (FOIP) was passed by the Legislative Assembly in 1992. It is 23 years old and has had only minor amendments. *The Local Authority Freedom of Information and Protection of Privacy Act* (LA FOIP) was passed in 1993 and is 22 years old. Similarly, it has had only minor amendments. It is time that these two statutes be reviewed and amended to bring them up to date. The updating of a statute gives the legislators an opportunity to recognize court decisions, clarify interpretations and take account of current developments in access & privacy law.

This document sets out a series of proposed amendments to FOIP and LA FOIP and the amendments are placed in four categories, those that:

- benefit "citizens";
- benefit "public bodies";
- will assist the "Commissioner"; and
- are of a "general" nature.

The proposals attempt to achieve a number of objectives:

- shortening timelines so that citizens get information or decisions sooner
- creating a similar process for reviews of access requests and investigations of breaches of privacy
- clarification of provisions
- recognition of electronic communications
- efficiencies to save time and taxpayers dollars
- making provisions similar to Alberta and British Columbia so that provisions are closer to harmonize in Western Canada

This list of proposed amendments has been developed based on experience of the Information and Privacy Commissioner's Office, public bodies and developments in information and privacy law across Canada.

This document does not propose amendments to *The Health Information Protection Act* (HIPA), but when HIPA is reviewed, some of the requested amendments would be appropriate for HIPA also.

Since HIPA was drafted later than FOIP and LA FOIP, some of its provisions are more precise and clearer, so in some instances the proposals involved putting HIPA language in FOIP and LA FOIP. This would also have the advantage of having similar wording in all three statutes which will lead to less confusion on the part of those reading and applying the legislation.

SUMMARY OF PROPOSALS

Part I Amendments for Citizens

1. Object or Purpose Clause - There is presently no object or purpose clause in FOIP or LA FOIP. It is proposed the Acts have a purpose clause.

2. Definition of "Government Institution" - FOIP presently defines "government institution", but new institutions need to be added by the Regulations. It is proposed that all government bodies or agencies be government institutions unless specifically exempted by the Regulations.

3. Definition of "Employee" - There is presently no definition of "employee" in the Acts. It is proposed that there be a definition of "employee" that includes contractors and agents.

4. Duty to Assist – The Acts do not contain an express provision regarding the duty to assist. A new section is proposed similar to that in HIPA.

5. Duty to Protect – The Acts do not contain an express provision regarding the duty to protect. A new section is proposed similar to that in HIPA.

6. Mandatory Breach Notification - There is presently no provision in the Acts regarding mandatory breach notification. This amendment provides direction to public bodies as to when notice of a privacy breach is to be reported to the Commissioner and the affected individuals.

7. Grounds for Review - It is proposed that the Acts be amended so that the Commissioner may review public bodies' decisions regarding the transfer of a request to another government institution, fee estimates, refusals to waive fees, any suspected privacy breach, allegations that a duty imposed was not performed by the public body or contravention of the Act.

8. Government Institution Response Time – It is proposed the Acts be amendment to reduce the government response time to access to information requests to 20 days from 30 days.

9. Record Will be Published – Presently, if the record will be published within 90 days, FOIP and LA FOIP allows for notice to be given to an Applicant that access is denied. It is proposed the Acts be amended to reduce the time period for publication to 20 days.

10. Manuals Made Available – It is proposed that a government institution (local authority) make their manuals available online electronically or in paper.

11. Open Government - Having to process access to information requests, including preparing fee estimates, is time consuming and expensive. A new section is proposed that would help clarify what type of government records should be proactively released outside of the formal application process.

12. Consultants and Contractors - FOIP and LA FOIP presently do not have language similar to that found in HIPA dealing with information management service providers. It is proposed that a new section be introduced into FOIP and LA FOIP partly modeled on section 18 of HIPA but drafted so as to cover IT providers and other contractors.

13. Third Party Personal Information – It is proposed to add a section providing an exemption for third party personal information. All provinces have such an exemption except Saskatchewan and Quebec.

14. Police a Local Authority – Saskatchewan and Prince Edward Island are the only provinces where the police are not bound by access and privacy legislation. It is proposed that municipal policing services be added as a local authority under LA FOIP.

Part II Amendments for Public Bodies

15. Frivolous or Vexatious Access Requests - It is proposed that Saskatchewan introduce a provision in FOIP and LA FOIP similar to that used in Alberta that would enable the Commissioner to authorize a public body to disregard one or more access to information requests if repetitious, frivolous or vexatious.

16. Recovery of Personal Information – It is proposed that an amendment to grant the necessary authority for public bodies to take the necessary action to retrieve personal information that may end up in the wrong hands.

17. Other Forms of Privilege Not Captured - Currently, only solicitor client privilege is covered by FOIP and LA FOIP. It is proposed that FOIP and LA FOIP be amended to provide for any type of legal privilege including litigation privilege and a section be introduced similar to that in Alberta.

18. Abandoned Requests – It is proposed there be clarification as to when applications may be deemed abandoned.

19. Publicly Available Information - In order to clarify when a government institution can obtain or use publicly available information, we have proposed language to clarify the point.

Part III Amendments to Assist the Commissioner

20. Grounds to Refuse to do a Review - It is proposed that the Acts be amended to include additional grounds to refuse a review, such as: the request does not involve the individual personally; there is another alternate dispute mechanism or professional body that could be engaged; there is insufficient evidence; the public body already responded adequately; or, a report has already been issued on the subject.

21. Production of Documents - It is proposed that the Acts be amended to require the public body to provide the Commissioner with the requested documents within 20 days.

22. Notice of Intention to Review - Presently, the Acts require the Commissioner to give public bodies 30 days notice before commencing a review or investigation. It is proposed to delete the 30 day notice and allow the review or investigation to start right away.

23. Determine Own Procedures - Presently the Acts are silent on the issue of establishing procedures for reviews or investigations. It is proposed to include language similar to that in the federal *Privacy Act*.

24. Cross-jurisdictional Investigations - It is proposed that the Acts have a section similar to Alberta to enable information sharing with other oversight bodies when an investigation involves more than one jurisdiction.

25. Conflict of Interest of Commissioner - In cases of conflict of interest of the Commissioner, it is proposed that the Acts be amendment to authorize delegation to a staff member.

26. Issuing Reports – It is proposed that the Acts be amended to say the Commissioner "may" issue a report. There are instances such as early resolution, where discretion could be exercised to not issue a report.

27. Response by the Head – It is proposed that government institutions or local authorities respond to the Commissioner's reports in 20 days.

28. Appeals – It is proposed that the Acts be amended to allow the Commissioner to intervene and make representations to the Court.

29. Offences Under the Act – This amendment would allow the Commissioner to be a witness or provide documents where there is an offense under the Act.

30. Offence Provisions in FOIP and LA FOIP - The offence language in the Acts should be amended to mirror that found in HIPA regarding employees caught snooping and contain a provision similar to a proposed amendment in Ontario's *Personal Health Information Protection Act* (PHIPA).

31. Privacy Impact Assessment (PIA) - In order to ensure that privacy protective practices are embedded in program design at the beginning, we believe PIAs should be mandatory in some cases. It is proposed the Acts have a provision that makes it clear when this should occur.

Part IV General

32. Statutes Subject to FOIP and LA FOIP – It is suggested there be a careful review of the present list of exemptions and, where an Act or a part of an Act is exempted, consideration be given to narrowing the exemption.

33. Five Year Review - In order to ensure that the Acts are reviewed regularly, it is proposed the Acts be amended to make it mandatory every five years.

34. Saskatchewan's Private Sector Employees - It is proposed that legislation be introduced to provide protection to employees in the private sector similar to the protection employees have in the public sector.

35. Consolidation of FOIP/LA FOIP – It is proposed the Acts be merged to eliminate confusion as to which Act applies and to address discrepancies between the two.

PART I
AMENDMENTS FOR CITIZENS

1. Object or Purpose Clause

Some privacy legislation sets out the purposes of the legislation at the beginning of the Act. Such purposes help those interpreting and applying the Act. When dealing with legislation that is quasi constitutional, it is important to have a clear statement of purposes for heads, the Commissioner and the Courts to refer to.

In Alberta's *Freedom of Information and Protection of Privacy Act* (AB FOIP) the purposes are set out as follows:

> **Purposes of this Act**
> 2 The purposes of this Act are
>
> (a) to allow any person a right of access to the records in the custody or under the control of a public body subject to limited and specific exceptions as set out in this Act,
>
> (b) to control the manner in which a public body may collect personal information from individuals, to control the use that a public body may make of that information and to control the disclosure by a public body of that information,
>
> (c) to allow individuals, subject to limited and specific exceptions as set out in this Act, a right of access to personal information about themselves that is held by a public body,
>
> (d) to allow individuals a right to request corrections to personal information about themselves that is held by a public body, and
>
> (e) to provide for independent reviews of decisions made by public bodies under this Act and the resolution of complaints under this Act.

British Columbia's *Freedom of Information and Protection of Privacy Act* (FIPPA) sets out its purposes as follows:

> **Purposes of this Act**
> 2 (1) The purposes of this Act are to make public bodies more accountable to the public and to protect personal privacy by
>
> (a) giving the public a right of access to records,
>
> (b) giving individuals a right of access to, and a right to request correction of, personal information about themselves,
>
> (c) specifying limited exceptions to the rights of access,

(d) preventing the unauthorized collection, use or disclosure of personal information by public bodies, and

(e) providing for an independent review of decisions made under this Act.

The federal *Access to Information Act* (AIA) provides as follows*:*

Purpose
2(1) The purpose of this Act is to extend the present laws of Canada to provide a right of access to information in records under the control of a government institution in accordance with the principles that government information should be available to the public, that necessary exceptions to the right of access should be limited and specific and that decisions on the disclosure of government information should be reviewed independently of government.

HIPA has the following preamble:

WHEREAS the Legislative Assembly recognizes the following principles with respect to personal health information:

THAT personal health information is private and shall be dealt with in a manner that respects the continuing interests of the individuals to whom it relates;

THAT individuals provide personal health information with the expectation of confidentiality and personal privacy;

THAT trustees of personal health information shall protect the confidentiality of the information and the privacy of the individuals to whom it relates;

THAT the primary purpose of the collection, use and disclosure of personal health information is to benefit the individuals to whom it relates;

THAT, wherever possible, the collection, use and disclosure of personal health information shall occur with the consent of the individuals to whom it relates;

THAT personal health information is essential to the provision of health services;

THAT, wherever possible, personal health information shall be collected directly from the individual to whom it relates;

THAT personal health information shall be collected on a need-to-know basis;

THAT individuals shall be able to obtain access to records of their personal health information;

THAT the security, accuracy and integrity of personal health information shall be protected;

THAT trustees shall be accountable to individuals with respect to the collection,

use, disclosure and exercise of custody and control of personal health information;

THAT trustees shall be open about policies and practices with respect to the collection, use and disclosure of personal health information;

Proposal

It is proposed that FOIP and LA FOIP be amended to introduce a purposes section similar to that used in Alberta with wording such as the following:

XX The purposes of this Act are

(a) to allow any person a right of access to the records in the possession or under the control of a government institution (local authority) subject to limited and specific exemptions as set out in this Act;

(b) to control the manner in which a government institution (local authority) may collect personal information from individuals, to control the use that a government institution (local authority) may make of that information and to control the disclosure by a government institution (local authority) of that information;

(c) to allow individuals, subject to limited and specific exemptions as set out in this Act, a right of access to personal information about themselves that is held by a government institution (local authority);

(d) to allow individuals a right to request corrections to personal information about themselves that is held by a government institution (local authority); and

(e) to provide for independent reviews of decisions made by government institutions (local authorities) under this Act and the resolution of complaints under this Act.

2. Definition of "Government Institution"

Government creates many organizations, agencies, and corporations to do its work (it is no longer just executive council and ministries). Government sometimes converts an organization into a corporation, agency or other body. It is difficult to always ensure that all entities are prescribed as "government institutions". For example, the Public Guardian and Trustee was not a government institution until it was prescribed in the FOIP Regulations. In Review Report 056-2014, the Office of the Chief Coroner was found not to be a "government institution" just because of the technical wording of subsection 2(1)(d). In the FOIP Regulations, section 3 creates an Appendix listing all the prescribed institutions. There are 74 names on that list. This Appendix must be regularly amended to keep up with changes in organizations.

In Newfoundland, the *Access to Information and Protection of Privacy Act* (ATIPPA) provides:

Definitions
2. In this Act
…

(p) "public body" means

(i) a department created under the *Executive Council Act* , or a branch of the executive government of the province,

...

(v) the House of Assembly and statutory offices, as defined in the *House of Assembly Accountability, Integrity and Administration Act*, and

includes a body designated for this purpose in the regulations made under section 73, but does not include,

...

(viii) a body listed in the Schedule;

…

(s) "Schedule" means the schedule of bodies excluded from the definition of public body; and

Proposal

I note Newfoundland has taken the approach of excluding specified public bodies. I propose the similar approach where all government created organizations would be "government institutions" unless specifically exempted by regulation. This would ensure that new organizations would be caught by FOIP unless a conscious decision was made to exempt them.

It is proposed the following wording for subsection 2(1)(d):

(d) **"government institution"** means, subject to subsection (2):

(i) the office of Executive Council or any ministry, secretariat or other similar agency of the executive government of Saskatchewan; or

(ii) any Crown corporation, subsidiary of a Crown corporation;

(iii) any board, commission, office or agency created by a statute; or

(iv) any board, commission, corporation, agency, office or other body, whose members or directors are appointed, in whole or in part:

(A) by the Lieutenant Governor in Council;

(B) by a member of the Executive Council; or

(C) in the case of:

(I) a board, commission or other body, by a Crown corporation; or

(II) a Crown corporation, by another Crown corporation;

unless specifically excluded in the regulations.

3. Definition of "Employee"

There is presently no definition of employee in FOIP or LA FOIP.

Alberta's FOIP provides:

> **Definitions**
> 1 In this Act,
> …
> (e) "employee", in relation to a public body, includes a person who performs a service for the public body as an appointee, volunteer or student or under a contract or agency relationship with the public body;

Proposal

Several sections within FOIP and LA FOIP reference employees. Therefore, to assist in the interpretation of these sections, it is proposed that a definition of "employee" be added in section 2 of FOIP and LA FOIP similar to the definition in Alberta. With wording such as:

> 2(k) "employee", in relation to government institution (local authority), includes a person who performs a service for the government institution (local authority) as an appointee, officer, volunteer or student or under a contract or agency relationship with the government institution (local authority);

4. Duty to Assist

Presently, there is no explicit duty to assist in FOIP or LA FOIP, but HIPA states the following:

> **Duty to assist**
> **35**(1) Subject to sections 36 to 38, a trustee shall respond to a written request for access openly, accurately and completely.
>
> (2) On the request of an applicant, a trustee shall:
>
> (a) provide an explanation of any term, code or abbreviation used in the personal health information; or
>
> (b) if the trustee is unable to provide an explanation in accordance with clause (a), refer the applicant to a trustee that is able to provide an explanation.

Alberta's FOIP provides:

> **Duty to assist applicants**
> **10**(1) The head of a public body must make every reasonable effort to assist applicants and to respond to each applicant openly, accurately and completely.
>
> (2) The head of a public body must create a record for an applicant if

(a) the record can be created from a record that is in electronic form and in the custody or under the control of the public body, using its normal computer hardware and software and technical expertise, and

(b) creating the record would not unreasonably interfere with the operations of the public body.

It was stated in the office's Review Report 2004-003:

> [12] There is no explicit duty to assist applicants in the Saskatchewan *Freedom of Information and Protection of Privacy Act*. Such an explicit duty exists in certain other provinces. For example, in the British Columbia *Freedom of Information and Protection of Privacy Act* the head of a public body "must make every reasonable effort to assist applicants and to respond without delay to each applicant openly, accurately and completely". [section 6(1)] A similar provision appears in the Alberta *Freedom of Information and Protection of Privacy Act* [section 10(1)].

Proposal

To be clear as to the pubic body's responsibility when processing access to information requests, it is proposed that a duty to assist be introduced into FOIP and LA FOIP similar to that in HIPA with wording such as the following:

> **XX** (1) Subject to other provisions in the act, a government institution (local authority) shall respond to a written request for access openly, accurately and completely.
>
> (2) On the request of an applicant, a government institution (local authority) shall:
>
> (a) provide an explanation of any term, code or abbreviation used in the record; or
>
> (b) if the government institution (local authority) is unable to provide an explanation in accordance with clause (a) refer the applicant to a government institution that is able to provide an explanation.

5. Duty to Protect

FOIP or LA FOIP do not have a section with a duty to protect but HIPA has the following provisions:

> **Duty to protect**
> **16** Subject to the regulations, a trustee that has custody or control of personal health information must establish policies and procedures to maintain administrative, technical and physical safeguards that will:
>
> (a) protect the integrity, accuracy and confidentiality of the information;
>
> (b) protect against any reasonably anticipated:

(i) threat or hazard to the security or integrity of the information;

(ii) loss of the information; or

(iii) unauthorized access to or use, disclosure or modification of the information; and

(c) otherwise ensure compliance with this Act by its employees.

Alberta's FOIP provides:

Protection of personal information
38 The head of a public body must protect personal information by making reasonable security arrangements against such risks as unauthorized access, collection, use, disclosure or destruction.

Similarly, British Columbia's FIPPA states:

Protection of personal information
30 A public body must 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.

Proposal

It is proposed that FOIP and LA FOIP have a section which provides a duty to protect similar to that in HIPA which might provide as follows:

XX Subject to the regulations, a government institution (local authority) shall protect personal information in its possession or under its control and must establish policies and procedures to maintain administrative, technical and physical safeguards that will:

(a) protect the integrity, accuracy and confidentiality of the information;

(b) protect against any reasonably anticipated:

(i) threat or hazard to the security or integrity of the information;

(ii) loss, damage or destruction of the information; or

(iii) unauthorized access to or use, disclosure or modification of the information; and

(c) otherwise ensure compliance with this Act by its employees, volunteers and students.

6. Mandatory Breach Notification

Breaches of personal information have been occurring more frequently. North America is moving to ensure that individuals are notified when a breach occurs.

There are two considerations with mandatory breach notification: (1) when to notify affected individuals; and (2) when to notify the Commissioner.

The following is from the Privacy Commissioner of Canada's submission to the senate standing committee on Transport and Communications on Bill S-4, An Act to amend *The Personal Information Protection and Electronic Documents Act* (PIPEDA) on the issue of breach notification:

> Background
> Bill S-4 amends many provisions in PIPEDA. On the whole, the proposed amendments will strengthen the privacy rights of Canadians with respect to their interactions with private sector companies, improve accountability and provide incentives for organizations to comply with the law. In particular, we welcome proposals to introduce a mandatory breach notification regime, and the compliance agreement provisions that will make it easier for our Office to ensure that companies meet the commitments they have made during investigations.
> …
>
> Breach Notification
> S-4 adds three new sections to PIPEDA: 10.1, 10.2 and 10.3, dealing with "Breaches of Security Safeguards". An organization that has experienced a breach of security safeguards involving personal information under its control will be required to provide notification in three circumstances:
>
> - to the Privacy Commissioner "if it is reasonable in the circumstances to believe that the breach creates a real risk of significant harm to an individual";
> - to the individuals whose personal information is involved "if it is reasonable in the circumstances to believe that the breach creates a real risk of significant harm to the individual"; and
> - to other organizations or government institutions if the notifying organization believes that the other organization or the government institution may be able to reduce the risk of harm that could result from the data breach or mitigate that harm.
>
> The definitions section defines a breach of security safeguards as "the loss of, unauthorized access to or unauthorized disclosure of personal information resulting from a breach of an organization's security safeguards that are referred to in clause 4.7 of Schedule 1 or from a failure to establish those safeguards."
>
> We strongly support these provisions. During the last few years we have seen a number of high profile data breaches both in Canada and abroad that compromised the personal information of Canadians. These provisions will create an incentive for organizations to take information security more seriously. In addition, they will provide individuals with

information that will help them mitigate the risks resulting from the loss or unauthorized access of their personal information.

Implementing mandatory breach notification provisions will bring PIPEDA into line with many other jurisdictions:

- Alberta's *Personal Information Protection Act* (PIPA) and some provincial personal health information protection acts contain mandatory breach notification;
- Almost every state in the United States has legislation making notification of individuals mandatory in certain circumstances; and
- The recently revised OECD Guidelines *Governing the Protection of Privacy and Transborder Flows of Personal Data* contain a breach notification recommendation.

The *Digital Privacy Act* proposes to amend PIPEDA as follows:

10.1 (1) An organization shall report to the Commissioner any breach of security safeguards involving personal information under its control if it is reasonable in the circumstances to believe that the breach creates a real risk of significant harm to an individual.

(2) The report shall contain the prescribed information and shall be made in the prescribed form and manner as soon as feasible after the organization determines that the breach has occurred.

(3) Unless otherwise prohibited by law, an organization shall notify an individual of any breach of security safeguards involving the individual's personal information under the organization's control if it is reasonable in the circumstances to believe that the breach creates a real risk of significant harm to the individual.

(4) The notification shall contain sufficient information to allow the individual to understand the significance to them of the breach and to take steps, if any are possible, to reduce the risk of harm that could result from it or to mitigate that harm. It shall also contain any other prescribed information.

(5) The notification shall be conspicuous and shall be given directly to the individual in the prescribed form and manner, except in prescribed circumstances, in which case it shall be given indirectly in the prescribed form and manner.

(6) The notification shall be given as soon as feasible after the organization determines that the breach has occurred.

(7) 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.

(8) The factors that are relevant to determining whether a breach of security safeguards creates a real risk of significant harm to the individual include

(a) the sensitivity of the personal information involved in the breach;

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

(c) any other prescribed factor.

10.2 (1) An organization that notifies an individual of a breach of security safeguards under subsection 10.1(3) shall notify any other organization, a government institution or a part of a government institution of the breach if the notifying organization believes that the other organization or the government institution or part concerned may be able to reduce the risk of harm that could result from it or mitigate that harm, or if any of the prescribed conditions are satisfied.

(2) The notification shall be given as soon as feasible after the organization determines that the breach has occurred.

(3) In addition to the circumstances set out in subsection 7(3), for the purpose of clause 4.3 of Schedule 1, and despite the note that accompanies that clause, an organization may disclose personal information without the knowledge or consent of the individual if

(a) The disclosure is made to the other organization, the government institution or the part of a government institution that was notified of the breach under subsection (1); and

(b) The disclosure is made solely for the purposes of reducing the risk of harm to the individual that could result from the breach or mitigating that harm.

(4) Despite clause 4.5 of Schedule 1, an organization may disclose personal information for purposes other than those for which it was collected in the circumstance set out in subsection (3).

10.3 (1) An organization shall, in accordance with any prescribed requirements, keep and maintain a record of every breach of security safeguards involving personal information under its control.

(2) An organization shall, on request, provide the Commissioner with access to, or a copy of, a record.

11. (1) An individual may file with the Commissioner a written complaint against an organization for contravening a provision of Division 1 or 1.1 or for not following a recommendation set out in Schedule 1.

Nova Scotia's *Personal Health Information Act* (PHIA) has a section on reporting of a privacy breach. It provides as follows:

69 Subject to the exceptions and additional requirements, if any, that are prescribed, a custodian that has custody or control of personal health information about an individual

shall notify the individual at the first reasonable opportunity if the custodian believes on a reasonable basis that

(a) the information is stolen, lost or subject to unauthorized access, use, disclosure, copying or modification; and

(b) as a result, there is potential for harm or embarrassment to the individual.

70 (1) Where a custodian determines on a reasonable basis that personal health information has been stolen, lost or subject to unauthorized access, use, disclosure, copying or modification, but

(a) it is unlikely that a breach of the personal health information has occurred; or

(b) there is no potential for harm or embarrassment to the individual as a result, the custodian may decide that notification to the individual pursuant to Section 69 is not required.

(2) Where a custodian makes the decision not to notify an individual pursuant to this Section, the custodian shall notify the Review Officer as soon as possible.

Alberta's PIPA states as follows:

Notification of loss or unauthorized access or disclosure
34.1(1) An organization having personal information under its control must, without unreasonable delay, provide notice to the Commissioner of any incident involving the loss of or unauthorized access to or disclosure of the personal information where a reasonable person would consider that there exists a real risk of significant harm to an individual as a result of the loss or unauthorized access or disclosure.

(2) A notice to the Commissioner under subsection (1) must include the information prescribed by the regulations.

Ontario's *Personal Health Information Protection Act* (PHIPA) provides as follows:

Notice of loss, etc.
12(2) Subject to subsection (3) and subject to the exceptions and additional requirements, if any, that are prescribed, a health information custodian that has custody or control of personal health information about an individual shall notify the individual at the first reasonable opportunity if the information is stolen, lost, or accessed by unauthorized persons.

Proposal

It is proposed to have wording similar to Alberta's which might provide as follows:

XX(1) For the purposes of this section, unauthorized access means a government institution (local authority) having personal information in its possession or under its control shall, without unreasonable delay, provide notice to the Commissioner of any incident involving the loss of or unauthorized use or disclosure of the personal

information where a reasonable person would consider that there exists a real risk of significant harm to an individual as a result of the loss or unauthorized use or disclosure.

(2) A notice to the Commissioner under subsection (1) shall include the information prescribed by the regulations.

7. Grounds for a Review

Presently, the reviewable grounds in FOIP are as follows:

> **Application for review**
> **49**(1) Where:
>
> (a) an applicant is not satisfied with the decision of a head pursuant to section 7, 12 or 37;
>
> (b) a head fails to respond to an application for access to a record within the required time; or
>
> (c) an applicant requests a correction of personal information pursuant to clause 32(1)(a) and the correction is not made;
>
> the applicant may apply in the prescribed form and manner to the commissioner for a review of the matter.

Section 7 referred to above deals with "response required" (i.e. access denied, records do not exist, record will be published), section 12 deals with time extensions and section 37 relates to decisions involving third parties.

LA FOIP has a similarly worded provision in section 38.

In IPC Review Report 2005-005 the Commissioner decided he could review fees:

> **3. Is the Commissioner Entitled to Review a Fee Estimate/Fees?**
>
> [26] The Act does not expressly provide for a review of fees or a fee estimate by the Information and Privacy Commissioner. We note however that in Report 2000/029, former Commissioner Gerald Gerrand concluded that, *"In my view, Section 7(2)(a) The Freedom of Information and Protection of Privacy Act allows me to review the decision of a head of a government department regarding the fee applicable with respect to an application.*" In that case Mr. Gerrand was dealing with a fee estimate from SPMC.

In Ontario, the *Freedom of Information and Protection of Privacy Act* (FIPPA) provides:

> **Review**
> **57**(5) A person who is required to pay a fee under subsection (1) may ask the Commissioner to review the amount of the fee or the head's decision not to waive the fee.

In Newfoundland, ATIPPA provides:

> **Complaints**
> **44**(1) The commissioner may investigate and attempt to resolve complaints that
> …
> (b) a fee required under this Act is inappropriate.

Prince Edward Island's (PEI) *Freedom of Information and Protection of Privacy Act* (FOIPP) has a similarly worded provision as follows:

> **50**(2) Without limiting subsection (1), the Commissioner may investigate and attempt to resolve complaints that
> …
> (c) a fee required under this Act is inappropriate;

General language found in Alberta's FOIP dealing with Commissioner's Orders states the following:

> **72**(3) If the inquiry relates to any other matter, the Commissioner may, by order, do one or more of the following:
>
> (a) require that a duty imposed by this Act or the regulations be performed;
> …
> (c) confirm or reduce a fee or order a refund, in the appropriate circumstances, including if a time limit is not met;

The Office reviewed the transfer of an access request in Review Report F-2013-005 but it is not clear that the Commissioner has authority to do so.

Proposal

It is proposed to amend section 49 of FOIP and section 38 of LA FOIP to include review of transfer to another institution, fees, fee estimates and refusal to waive fees.

Further, if wording were included such as "any contravention to the Act" as it is in section 42 of HIPA, the ability to review any contravention of the Act would be much clearer.

HIPA, in section 42 provides:

> **Application for review**
> **42**(1) A person may apply to the commissioner for a review of the matter where:
> …
> (c) the person believes that there has been a contravention of this Act.

HIPA makes it clear that a person can request a review where he or she believes there is a contravention of HIPA.

Finally, the Act should be made clear that the Commissioner can review any alleged breach of privacy or release of personal information.

It is proposed that wording be added to section 49 of FOIP (section 38 LA FOIP) as follows:

> **Application for Review and Investigation**
> **49**(1) Where:
>
> …
>
> (d) the applicant believes that his or her personal information has been improperly collected, used or disclosed;
>
> (e) the applicant is not satisfied that a reasonable fee was charged;
>
> (f) the applicant believes that the fee should have been waived;
>
> (g) the applicant believes the access request was not properly transferred to another government institution (local authority);
>
> (h) the applicant is not satisfied that a duty imposed by this act or the regulations was performed; or
>
> (i) the applicant believes there has been a contravention of this act or the regulations;
>
> the applicant may apply in the prescribed form and manner to the Commissioner for a review and investigation of the matter.

8. Government Institution Response Time

In today's electronic age, waiting 30 days for the record is just too long. If the record is 1, 2, 3 or 5 pages, it certainly does not take 30 days to locate it, review and send it out or claim an exemption. It would be an improvement to the system to require responses in 20 days with an exception for longer records or difficult situations.

Quebec has a requirement of 20 days.

Proposal

It is proposed to amend section 7 to require a response in 20 days.

9. Record Will be Published

In subsection 7(2)(c) of FOIP and subsection 7(2)(c) of LA FOIP it provides that the head can respond that the records will be published in 90 days. With today's web sites and the ease of publication, it is reasonable now to shorten this time. Thirty days seems reasonable. FOIP now provides:

Response required
7(2) The head shall give written notice to the applicant within 30 days after the application is made:

…

(c) if the record is to be published within 90 days, informing the applicant of that fact and of the approximate date of publication;

LA FOIP section 7 has similar wording.

Newfoundland's ATIPPA splits the above time period in half as follows:

Published material
14(1) The head of a public body may refuse to disclose a record or part of a record that

…

(b) is to be published or released to the public within 45 days after the applicant's request is received.

(2) The head of a public body shall notify an applicant of the publication or release of information that the head has refused to give access to under paragraph (1)(b).

(3) Where the information is not published or released within 45 days after the applicant's request is received, the head of the public body shall reconsider the request as if it were a new request received on the last day of that period, and access may not be refused under paragraph (1) (b).

Proposal

It is proposed to amend subsection 7(2)(c) of FOIP (subsection 7(2)(c) LA FOIP) to require publication within 20 days.

10. Manuals Made Available

Currently manuals of government institutions are to be made available to a citizen in the offices of the institution. Subsection 65(1) of FOIP provides:

Access to manuals
65(1) Within two years after this section comes into force, every head shall provide facilities at:

(a) the headquarters of the government institution; and

(b) any offices of the government institution that, in the opinion of the head, are reasonably practicable;

where the public may inspect any manual, handbook or other guide-line used in decision-making processes that affect the public by employees of the government institution in administering or carrying out programs or activities of the government institution.

No similar provision exists in LA FOIP.

In today's world there is no justification in requiring a citizen to come to an office of the government institution or local authority. Best practice would suggest the manuals, policies and guidelines would be placed on the organization's web site. In many cases that is what occurs now.

Proposal

It is proposed that section 65 of FOIP be amended to reflect current practices and technology and a similar new section be placed in LA FOIP as follows:

> **65**(1) Every government institution (local authority) shall make available on their web site all manuals, policies, guidelines or procedures that are used in decision-making processes that affect the public by employees of the government institution (local authority) in administering or carrying out programs or activities of the government institution (local authority), or alternatively, provide such when requested in electronic or paper form.

11. Open Government

In fiscal year 2013-2014, the government received approximately 2200 access requests. Some of those requests were of a similar nature, for example, travel expenses of officials. The Commissioner has set a five year goal to promote public bodies making information available which is frequently requested. The City of Regina has adopted an open information strategy by publishing commonly requested data, citizens get the information quickly and the public body does not have to respond to numerous access requests.

In a submission entitled "Becoming a Leader in Access and Privacy" to the 2013 Government of Alberta FOIP Act Review by the Alberta Information and Privacy Commissioner, it stated:

> Darbishire's Working Paper cites access to information legislation in jurisdictions such as Mexico and India as examples in which specific classes of information are identified for proactive disclosure without the need for access to information requests. Mexico, Slovenia and the United States are also noted as jurisdictions in which public bodies are required to proactively disclose frequently requested records. (http://www.oipc.ab.ca/Content_Files/Files/Publications/FOIP_Act_Review_2013_Becoming_A_Leader.pdf)
>
> In some jurisdictions (e.g. the United States, Mexico) access to information laws require the information be made available electronically. (http://www.oipc.ab.ca/Content_Files/Files/Publications/FOIP_Act_Review_2013_Becoming_A_Leader.pdf)

FOIP and LA FOIP presently have nothing in their legislation that promotes open access strategies.

British Columbia's FIPPA has a provision as follows:

> **Records available without request**
> **71** (1) Subject to subsection (1.1), the head of a public body must establish categories of records that are in the custody or under the control of the public body and are available to the public without a request for access under this Act.
>
> (1.1) The head of a public body must not establish a category of records that contain personal information unless the information
>
> (a) may be disclosed under section 33.1 or 33.2, or
>
> (b) would not constitute, if disclosed, an unreasonable invasion of the personal privacy of the individual the information is about.
>
> (1.2) Section 22 (2) to (4) applies to the determination of unreasonable invasion of personal privacy under subsection (1.1) (b) of this section.
>
> (2) The head of a public body may require a person who asks for a copy of an available record to pay a fee to the public body.
>
> (3) Subsection (1) does not limit the discretion of the government of British Columbia or a public body to disclose records that do not contain personal information.
>
> **Records that ministries must disclose**
> **71.1** (1) Subject to subsection (2), the minister responsible for this Act may establish categories of records that are in the custody or under the control of one or more ministries and are available to the public without a request for access under this Act.
>
> (2) The minister responsible for this Act must not establish a category of records that contain personal information unless the information
>
> (a) may be disclosed under section 33.1 or 33.2, or
>
> (b) would not constitute, if disclosed, an unreasonable invasion of the personal privacy of the individual the information is about.
>
> (3) Section 22 (2) to (4) applies to the determination of unreasonable invasion of personal privacy under subsection (2) (b) of this section.
>
> (4) The minister responsible for this Act may require one or more ministries to disclose a record that is within a category of records established under subsection (1) of this section or section 71 (1).
>
> (5) If required to disclose a record under subsection (4), a ministry must do so in accordance with any directions issued relating to the disclosure by the minister responsible for this Act.

Proposal

It is proposed that FOIP and LA FOIP have sections similar to British Columbia's section 71 which would promote and encourage open information strategies. The section might provide as follows:

> **XX** (1) Subject to subsection (2), the head of a government institution (local authority) may establish categories of records that are in the possession or under the control of the government institution (local authority) and are available to the public within a reasonable time without a request for access under this Act.
>
> (2) The head of a government institution (local authority) shall not establish a category of records that contain personal information unless that information may be disclosed under this Act or the regulations.

12. Consultants and Contractors

Today government institutions and local authorities may have to, in order to carry out their mandate, contract with consultants, advisers, professionals or IT specialists to obtain services. In that process the contractor receives, stores or becomes aware of personal information. That personal information in the custody or control of a contractor deserves the same protection it has in the custody of the government institution or local authority.

HIPA recognizes this fact. It first has a definition of a "trustee" which certainly includes professionals and private businesses. Trustee includes personal care homes, labs and pharmacies. Second it refers to "health care organizations" and "information management service providers."

Section 18 of HIPA deals with information management service providers and provides as follows:

> **18**(1) A trustee may provide personal health information to an information management service provider:
>
> (a) for the purpose of having the information management service provider process, store, archive or destroy the personal health information for the trustee;
>
> (b) to enable the information management service provider to provide the trustee with information management or information technology services;
>
> (c) for the purpose of having the information management service provider take custody and control of the personal health information pursuant to section 22 when the trustee ceases to be a trustee; or
>
> (d) for the purpose of combining records containing personal health information.
>
> (2) **Not yet proclaimed.** Before providing personal health information to an information management service provider, a trustee must enter into a written agreement with the information management service provider that:

(a) governs the access to and use, disclosure, storage, archiving, modification and destruction of the information;

(b) provides for protection of the information; and

(c) meets the requirements of the regulations.

(3) An information management service provider shall not use, disclose, obtain access to, process, store, archive, modify or destroy personal health information received from a trustee except for the purposes set out in subsection (1).

(4) **Not yet proclaimed.** An information management service provider must comply with the terms of the agreement entered into pursuant to subsection (2).

(5) If a trustee is also an information management service provider and has received personal health information from another trustee in accordance with subsection (1), the trustee receiving the information is deemed to be an information management service provider for the purposes of that personal health information and does not have any of the rights and duties of a trustee with respect to that information.

The New Brunswick's *Personal Health Information Privacy and Access Act* requires custodians to enter into written agreements with information managers as follows:

Agents and information managers

52(1) A custodian that retains the services of an agent for the collection, use, disclosure or retention of person health information shall enter into a written agreement with the agent requiring the agent to comply with the custodian's legal obligations regarding handling of personal health information.

52(2) A custodian may provide personal health information to an information manager for the purpose of processing, storing or destroying the personal health information or providing the custodian with information management or information technology services.

52(3) A custodian that wishes to provide personal health information to an information manager shall enter into a written agreement with the information manager, in accordance with the regulations, that provides for the protection of the personal health information against risks such as unauthorized access to or use or disclosure, secure destruction or alteration of the information.

52(4) An information manager who enters into a written agreement under subsection (3) shall comply with

(a) he duties imposed on the information manager under the agreement, and

(b) the same requirements concerning the protection, retention and secure destruction of personal health information that the custodian is required to comply with under this Act.

Further, New Brunswick's *General Regulations-Personal Health Information Privacy and Access Act* include the following regarding the content of such agreements:

> **21** Information managers. – A written agreement for the provision of personal health information between a custodian and information manager referred to in subsection 52(3) of the Act shall describe
>
> (a) the services to be provided to the custodian, and
>
> (b) the administrative, technical and physical safeguards employed by the information manager relating to the confidentiality, security, accuracy and integrity of the personal health information.

Newfoundland and Labrador's *Personal Health Information Act* contains the following provision on information managers:

> **Information manager**
> **22.**(1) A custodian that retains the services of an information manager for the provision of a service described in paragraph 2(1)(l) shall enter into an agreement with the information manager in accordance with subsection (2).
>
> (2) An agreement referred to in subsection (1) shall be in writing and shall provide for the protection of the personal health information against unauthorized access, use, disclosure, disposition, loss or modification in accordance with this Act and the regulations.
>
> (3) An information manager to which personal health information is disclosed by the custodian may use or disclose that information only for the purpose authorized by the agreement.
>
> (4) An information manager shall comply with
>
> (a) this Act and the regulations; and
>
> (b) the terms of the agreement entered into with the custodian
>
> in respect of the personal health information disclosed to it under subsection (2).
>
> (5) An information manager shall not permit its employee or a person acting on its behalf to access the personal health information disclosed to it by the custodian unless the employee or person acting on its behalf agrees in writing to comply with this Act and the restrictions imposed upon the information manager referred to in subsection (4).
>
> (6) Nothing in subsection (4) or (5) relieves a custodian from its obligations under this Act and the regulations in respect of the personal health information disclosed by the custodian to the information manager, and the personal health information that has been disclosed to an information manager under an agreement under subsection (2) is considered to continue in the custody and control of the custodian for the purpose of this Act and the regulations.

(7) An information manager may, in accordance with the terms of an agreement with a custodian, construct or create an integrated electronic record of personal health information comprising individual records, the custody or control of each of which may be in one or more custodians.

Alberta's *Health Information Act* (HIA) requires the following when it comes to information managers:

Power to enter agreement with information manager

66(1) In this section, "information manager" means a person or body that

(a) processes, stores, retrieves or disposes of health information,

(b) in accordance with the regulations, strips, encodes or otherwise transforms individually identifying health information to create non-identifying health information, or

(c) provides information management or information technology services.

(2) A custodian must enter into a written agreement with an information manager in accordance with the regulations for the provision of any or all of the services described in subsection (1).

(3) A custodian that has entered into an agreement with an information manager may provide health information to the information manager without the consent of the individuals who are the subjects of the information for the purposes authorized by the agreement.

(4) An information manager to which information is provided pursuant to subsection (3) may use or disclose that information only for the purposes authorized by the agreement.

(5) An information manager must comply with

(a) this Act and the regulations, and

(b) the agreement entered into with a custodian

in respect of information provided to it pursuant to subsection (3).

(6) Despite subsection (5)(a), a custodian continues to be responsible for compliance with this Act and the regulations in respect of the information provided by the custodian to the information manager.

(7) A custodian that is an information manager for another custodian does not become a custodian of the health information provided to it in its capacity as an information manager, but nothing in this section prevents the custodian from otherwise collecting, using or disclosing that same health information in accordance with this Act.

Further, Alberta's *Health Information Regulation* spells out what must be contained in an information manager agreement as follows:

> **Information manager agreement**
> **7.2** For the purposes of section 66(2) of the Act, an agreement between a custodian and an information manager must
>
> (a) identify the objectives of the agreement and the principles to guide the agreement,
>
> (b) indicate whether or not the information manager is permitted to collect health information from any other custodian or from a person and, if so, describe that health information and the purpose for which it may be collected,
>
> (c) indicate whether or not the information manager may use health information provided to it by the custodian and, if so, describe that health information and the purpose for which it may be used,
>
> (d) indicate whether or not the information manager may disclose health information provided to it by the custodian and, if so, describe that health information and the purpose for which it may be disclosed,
>
> (e) describe the process for the information manager to respond to access requests under Part 2 of the Act or, if the information manager is not to respond to access requests, describe the process for referring access requests for health information to the custodian itself,
>
> (f) describe the process for the information manager to respond to requests to amend or correct health information under Part 2 of the Act or, if the information manager is not to respond to requests to amend or correct health information, describe the process for referring access requests to amend or correct health information to the custodian itself,
>
> (g) describe how health information provided to the information manager is to be protected, managed, returned or destroyed in accordance with the Act,
>
> (h) describe how the information manager is to address an expressed wish of an individual relating to the disclosure of that individual's health information or, if the information manager is not to address an expressed wish of an individual relating to the disclosure of that individual's health information, describe the process for referring these requests to the custodian itself, and
>
> (i) set out how an agreement can be terminated.

Manitoba's *Personal Health Information Act* (PHIA) includes the following:

> **Trustee may provide information to an information manager**
> **25**(1) A trustee may provide personal health information to an information manager for the purpose of processing, storing or destroying it or providing the trustee with information management or information technology services.

Restrictions on use
25(2) An information manager may use personal health information provided to it under this section only for the purposes and activities mentioned in subsection (1), which must be purposes and activities that the trustee itself may undertake.

Agreement required
25(3) A trustee who wishes to provide personal health 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 health information against such risks as unauthorized access, use, disclosure, destruction or alteration, in accordance with the regulations.

Information manager must comply with Act
25(4) An information manager shall comply with

(a) the same requirements concerning the protection, retention and destruction of personal health information that the trustee 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 trustee
25(5) Personal health information that has been provided to an information manager under an agreement described in subsection (3) is deemed to be maintained by the trustee for the purposes of this Act.

Proposal

It is proposed that a new section be introduced into FOIP and LA FOIP partly modeled on section 18 of HIPA but drafted so as to cover IT providers and other contractors. The section might provide as follows:

XX (1) A government institution (local authority) may provide personal information to an information management service provider or consultant:

(a) for the purpose of having the information management service provider process, store, archive or destroy the personal information for the government institution (local authority);

(b) to enable the information management service provider to provide the government institution (local authority) with information management or information technology services;

(c) for the purpose of having the information management service provider take custody and control of the personal information;

(d) for the purpose of combining records containing personal information; or

(e) for the purpose of providing consulting services.

(2) Before providing personal information to an information management service provider, contractor or consultant, a government institution (local authority) must enter into a written agreement with the information management service provider, contractor or consultant that:

(a) governs the access to and use, disclosure, storage, archiving, modification and destruction of the information;

(b) provides for protection of the information; and

(c) meets the requirements of the Act and regulations.

(3) An information management service provider, contractor or consultant shall not use, disclose, obtain access to, process, store, archive, modify or destroy personal information received from a government institution (local authority) except for the purposes set out in subsection (1).

(4) An information management service provider, contractor or consultant must comply with the terms of the agreement entered into pursuant to subsection (2).

13. Third Party Personal Information

All provinces and territories, except Quebec and Saskatchewan, have a third party personal information exemption. Currently, government institutions cite subsection 29(1) of FOIP (subsection 28(1) LA FOIP) as its reason to withhold third party personal information when preparing records for an access to information request. Subsection 29(1) of FOIP is a disclosure provision but is being used as an exemption.

Alberta's FOIP provides a third party personal information exemption. This exemption has four parts. First, it provides that a public body must not disclose third party personal information if the disclosure would be an unreasonable invasion of a third party's personal information. Second, it provides when a disclosure would not be an unreasonable invasion of privacy. Third, it provides when a disclosure would be presumed to be an unreasonable invasion of privacy. Finally, it provides circumstances that the head of a public body must consider when determining whether a disclosure is an unreasonable invasion of privacy. Alberta's FOIP provides as follows:

17(1) The head of a public body must refuse to disclose personal information to an applicant if the disclosure would be an unreasonable invasion of a third party's personal privacy.

(2) A disclosure of personal information is not an unreasonable invasion of a third party's personal privacy if

(a) the third party has, in the prescribed manner, consented to or requested the disclosure,

(b) there are compelling circumstances affecting anyone's health or safety and written notice of the disclosure is given to the third party,

(c) an Act of Alberta or Canada authorizes or requires the disclosure,

(d)…
(e) the information is about the third party's classification, salary range, discretionary benefits or employment responsibilities as an officer, employee or member of a public body or as a member of the staff of a member of the Executive Council,

(f) the disclosure reveals financial and other details of a contract to supply goods or services to a public body,

(g) the information is about a licence, permit or other similar discretionary benefit relating to

(i) a commercial or professional activity, that has been granted to the third party by a public body, or

(ii) real property, including a development permit or building permit, that has been granted to the third party by a public body, and the disclosure is limited to the name of the third party and the nature of the licence, permit or other similar discretionary benefit,

(h) the disclosure reveals details of a discretionary benefit of a financial nature granted to the third party by a public body,

(i) the personal information is about an individual who has been dead for 25 years or more, or

(j) subject to subsection (3), the disclosure is not contrary to the public interest and reveals only the following personal information about a third party:

(i) enrolment in a school of an educational body or in a program offered by a post-secondary educational body,
…
(iii) attendance at or participation in a public event or activity related to a public body, including a graduation ceremony, sporting event, cultural program or club, or field trip, or

(iv) receipt of an honour or award granted by or through a public body.

(3) The disclosure of personal information under subsection (2)(j) is an unreasonable invasion of personal privacy if the third party whom the information is about has requested that the information not be disclosed.

(4) A disclosure of personal information is presumed to be an unreasonable invasion of a third party's personal privacy if

(a) the personal information relates to a medical, psychiatric or psychological history, diagnosis, condition, treatment or evaluation,

(b) the personal information is an identifiable part of a law enforcement record, except to the extent that the disclosure is necessary to dispose of the law enforcement matter or to continue an investigation,

(c) the personal information relates to eligibility for income assistance or social service benefits or to the determination of benefit levels,

(d) the personal information relates to employment or educational history,

(e) the personal information was collected on a tax return or gathered for the purpose of collecting a tax,

(e.1) the personal information consists of an individual's bank account information or credit card information,

(f) the personal information consists of personal recommendations or evaluations, character references or personnel evaluations,

(g) the personal information consists of the third party's name when

(i) it appears with other personal information about the third party, or

(ii) the disclosure of the name itself would reveal personal information about the third party, or

(h) the personal information indicates the third party's racial or ethnic origin or religious or political beliefs or associations.

(5) In determining under subsections (1) and (4) whether a disclosure of personal information constitutes an unreasonable invasion of a third party's personal privacy, the head of a public body must consider all the relevant circumstances, including whether

(a) the disclosure is desirable for the purpose of subjecting the activities of the Government of Alberta or a public body to public scrutiny,

(b) the disclosure is likely to promote public health and safety or the protection of the environment,

(c) the personal information is relevant to a fair determination of the applicant's rights,

(d) the disclosure will assist in researching or validating the claims, disputes or grievances of aboriginal people,

(e) the third party will be exposed unfairly to financial or other harm,

(f) the personal information has been supplied in confidence,

(g) the personal information is likely to be inaccurate or unreliable,

(h) the disclosure may unfairly damage the reputation of any person referred to in the record requested by the applicant, and

(i) the personal information was originally provided by the applicant.

Proposal

It is proposed that subsections 24(2) of FOIP (subsection 23(2) LA FOIP) be repealed. It is proposed that a new section 23.1 be added to include an exemption that is for third party personal information that is similar to Alberta's. The wording might be as follows:

23.1(1) The head of a government institution (local authority) shall refuse to disclose personal information to an applicant if the disclosure would be an unreasonable invasion of a third party's personal privacy.

(2) A disclosure of personal information is not an unreasonable invasion of a third party's personal privacy if:

(a) the third party has, in the prescribed manner, consented to or requested the disclosure,

(b) there are compelling circumstances affecting anyone's health or safety and written notice of the disclosure is given to the third party,

(c) an Act of the province or the parliament of Canada authorizes or requires the disclosure,

(d) the information is about the third party's classification, salary range, discretionary benefits or employment responsibilities as an officer, employee or member of a government institution (local authority) or as a member of the staff of a member of the Executive Council,

(e) the disclosure reveals financial and other details of a contract to supply goods or services to a government institution (local authority),

(f) the information is about a licence, permit or other similar discretionary benefit relating to

(i) a commercial or professional activity, that has been granted to the third party by a government institution (local authority), or

(ii) real property, including a development permit or building permit, that has been granted to the third party by a government institution (local authority), and the disclosure is limited to the name of the third party and the nature of the licence, permit or other similar discretionary benefit,

(g) the disclosure reveals details of a discretionary benefit of a financial nature granted to the third party by a government institution (local authority), or

(h) subject to subsection (3), the disclosure is not contrary to the public interest and reveals only the following personal information about a third party:

(i) enrolment in a school of an educational body or in a program offered by a post-secondary educational body,

(ii) attendance at or participation in a public event or activity related to a government institution (local authority), including a graduation ceremony, sporting event, cultural program or club, or field trip, or

(iii) receipt of an honour or award granted by or through a government institution (local authority).

(3) The disclosure of personal information under subsection (2)(h) is an unreasonable invasion of personal privacy if the third party whom the information is about has requested that the information not be disclosed.

(4) A disclosure of personal information is presumed to be an unreasonable invasion of a third party's personal privacy if:

(a) the personal information is an identifiable part of a law enforcement record, except to the extent that the disclosure is necessary to dispose of the law enforcement matter or to continue an investigation,

(b) the personal information relates to eligibility for income assistance or social service benefits or to the determination of benefit levels,

(c) the personal information relates to employment or educational history,

(d) the personal information was collected on a tax return or gathered for the purpose of collecting a tax,

(e) the personal information consists of an individual's bank account information or credit card information,

(f) the personal information consists of personal recommendations or evaluations, character references or personnel evaluations,

(g) the personal information consists of the third party's name when

(i) it appears with other personal information about the third party, or

(ii) the disclosure of the name itself would reveal personal information about the third party.

(h) the personal information indicates the third party's race, creed, religion, colour, sex, sexual orientation, family status or marital status, disability, age, nationality, ancestry, ethnic origin or political beliefs or associations.

(5) In determining under subsections (1) and (4) whether a disclosure of personal information constitutes an unreasonable invasion of a third party's personal privacy, the head of a government institution (local authority) shall consider all the relevant circumstances, including whether

(a) the disclosure is desirable for the purpose of subjecting the activities of the Government of Saskatchewan or a government institution (local authority) to public scrutiny,

(b) the disclosure is likely to promote public health and safety or the protection of the environment,

(c) the personal information is relevant to a fair determination of the applicant's rights,

(d) the disclosure will assist in researching or validating the claims, disputes or grievances of aboriginal people,

(e) the third party will be exposed unfairly to financial or other harm,

(f) the personal information has been supplied in confidence,

(g) the personal information is likely to be inaccurate or unreliable,

(h) the disclosure may unfairly damage the reputation of any person referred to in the record requested by the applicant, and

(i) the personal information was originally provided by the applicant.

14. Police a Local Authority

Currently police forces are not included as local authorities. All provinces except Saskatchewan and PEI include police forces in their access and privacy statutes (with appropriate exemptions). The RCMP is covered by the federal *Privacy Act* and *Access to Information Act*. One of the difficulties in working out proper privacy protections in Hubs is that municipal police forces are not covered by the same legislation that applies to government institutions, local authorities or trustees. There is a trend toward more information sharing between government institutions and local authorities in situations where vulnerable persons, including children, are at risk. These information sharing arrangements are going to be more complicated if municipal police forces are not governed by the same privacy laws.

Proposal

It is proposed to add the following to the definition of local authority in LA FOIP:

2(f) **"local authority"** means:

...

(xviii) a municipal police service as defined in the Police Act;

PART II
AMENDMENTS FOR PUBLIC BODIES

15. Frivolous or Vexatious Access Requests

From time to time public bodies have been faced with requests that are frivolous, repetitive, not understandable or vexatious. These can take a considerable amount of time to process. At the moment, public bodies cannot disregard an access to information request.

Alberta's FOIP has dealt with this issue in the following way:

> **Power to authorize a public body to disregard requests**
> **55**(1) If the head of a public body asks, the Commissioner may authorize the public body to disregard one or more requests under section 7(1) or 36(1) if
>
> (a) because of their repetitious or systematic nature, the requests would unreasonably interfere with the operations of the public body or amount to an abuse of the right to make those requests, or
>
> (b) one or more of the requests are frivolous or vexatious.
>
> (2) The processing of a request under section 7(1) or 36(1) ceases when the head of a public body has made a request under subsection (1) and
>
> (a) if the Commissioner authorizes the head of the public body to disregard the request, does not resume;
>
> (b) if the Commissioner does not authorize the head of the public body to disregard the request, does not resume until the Commissioner advises the head of the public body of the Commissioner's decision.

British Columbia has dealt with the issue in its FIPPA as follows:

> **Power to authorize a public body to disregard requests**
> **43**If the head of a public body asks, the commissioner may authorize the public body to disregard requests under section 5 or 29 that
>
> (a) would unreasonably interfere with the operations of the public body because of the repetitious or systematic nature of the requests, or
>
> (b) are frivolous or vexatious.

Proposal

It is proposed that Saskatchewan introduce a provision in FOIP and LA FOIP similar to that used in Alberta. The provision might provide as follows:

XX(1) If the head of a government institution (local authority) asks, the Commissioner may authorize the government institution (local authority) to disregard one or more requests under section 7 if:

(a) because of their repetitious or systematic nature, the requests would unreasonably interfere with the operations of the public body or amount to an abuse of the right of access to make those requests, or

(b) one or more of the requests are frivolous or vexatious.

(2) The processing of a request under section 7 ceases when the head of a government institution (local authority) has made a request under subsection (1) and:

(a) if the Commissioner authorizes the head of the government institution (local authority) to disregard the request, it does not resume;

(b) if the Commissioner does not authorize the head of the government institution (local authority) to disregard the request, it does not resume until the Commissioner advises the head of the government institution (local authority) of the Commissioner's decision.

16. Recovery of Personal Information

In the event of a privacy breach where personal information has fallen into the wrong hands, public bodies do not know what to do when it is necessary to retrieve or ensure the return or destruction of personal information.

In British Columbia's FIPPA, it is provided:

Recovery of personal information
73.1 (1) If the head of a public body has reasonable grounds to believe that personal information in the custody or under the control of the public body is in the possession of a person or an entity not authorized by law to possess the information, the head of the public body may issue a written notice demanding that person or entity to do either of the following within 20 calendar days of receiving the notice:

(a) return the information to the public body or, in the case of electronic records, securely destroy the information and confirm in writing the date and the means by which the information was securely destroyed;

(b) respond in writing and declare why the person or entity considers that

(i) the information was not in the custody or under the control of the public body when the person or entity acquired possession of the information, or

(ii) the person or entity is authorized by law to possess the information.

(2) The written notice referred to in subsection (1) must

(a) identify, with reasonable specificity, the personal information claimed to be in the custody or under the control of the public body and in the possession of the person or entity not authorized by law to possess the information, and

(b) state that the public body may undertake legal action to recover the personal information if the person or entity fails to respond in writing within the required time or does not adequately demonstrate that

(i) the information was not in the custody or under the control of the public body when the person or entity acquired possession of the information, or

(ii) the person or entity is authorized by law to possess the information.

Proposal

It is proposed that FOIP and LA FOIP have sections similar to British Columbia's section dealing with recovery of personal information and that it be made an offense not to return that personal information. The section might provide as follows:

XX (1) If the head of a government institution (local authority) has reasonable grounds to believe that personal information in the possession or under the control of the government institution (local authority) is in the possession of a person or an entity not authorized by law to possess the information, the head of the government institution (local authority) may issue a written notice demanding that person or entity to do either of the following within 20 days of receiving the notice:

(a) return the information to the government institution (local authority) or, in the case of electronic records, securely destroy the information and confirm in writing the date and the means by which the information was securely destroyed;

(b) respond in writing and declare why the person or entity considers that

(i) the information was not in the possession or under the control of the government institution (local authority) when the person or entity acquired possession of the information, or

(ii) the person or entity is authorized by law to possess the information.

(2) The written notice referred to in subsection (1) must:

(a) identify, with reasonable specificity, the personal information claimed to be in the possession or under the control of the government institution (local authority) and in the possession of the person or entity not authorized by law to possess the information, and

(b) state that the government institution (local authority) may undertake legal action to recover the personal information if the person or entity fails to respond in writing within the required time or does not adequately demonstrate that

(i) the information was not in the possession or under the control of the government institution (local authority) when the person or entity acquired possession of the information, or

(ii) the person or entity is authorized by law to possess the information.

17. Other Forms of Privilege Not Captured

Currently, only solicitor client privilege is covered by section 22 of FOIP and section 21 of LA FOIP. For instance, section 22 of FOIP provides as follows:

> **Solicitor-client privilege**
> **22** A head may refuse to give access to a record that:
>
> (a) contains information that is subject to solicitor-client privilege;
>
> (b) was prepared by or for an agent of the Attorney General for Saskatchewan or legal counsel for a government institution in relation to a matter involving the provision of advice or other services by the agent or legal counsel; or
>
> (c) contains correspondence between an agent of the Attorney General for Saskatchewan or legal counsel for a government institution and any other person in relation to a matter involving the provision of advice or other services by the agent or legal counsel.

Section 21 of LA FOIP has similar wording.

From Review Report 2005-002, the office noted the following on the topic of privilege:

> [35] We note that litigation privilege ends when the litigation is concluded however solicitor client privilege continues.
>
> [36] I recognize that in the Alberta legislation the exemption is broader than the solicitor client exemption in our section 22 …

The issue is dealt within Alberta's FOIP as follows:

> **Privileged information**
> **27**(1) The head of a public body may refuse to disclose to an applicant
>
> (a) information that is subject to any type of legal privilege, including solicitor-client privilege or parliamentary privilege,

Proposal

It is proposed that FOIP and LA FOIP be amended to provide for any type of legal privilege including litigation privilege and a section be introduced similar to that in Alberta.

18. Abandoned Requests

Sometimes Applicants can make an access request but when additional information is requested and there is a failure to follow through, or a fee is requested and the Applicant does not pay or indicate he or she will pay, the access request remains outstanding and cannot be completed. It is in the best interest of all to have access requests processed quickly and not to have access requests outstanding for an unreasonable length of time.

This issue is addressed in Alberta's FOIP as follows:

> **Abandoned request**
> **8**(1) Where the head of a public body contacts an applicant in writing respecting the applicant's request, including
>
> (a) seeking further information from the applicant that is necessary to process the request, or
>
> (b) requesting the applicant to pay a fee or to agree to pay a fee, and the applicant fails to respond to the head of the public body, as requested by the head, within 30 days after being contacted, the head of the public body may, by notice in writing to the applicant, declare the request abandoned.
>
> (2) A notice under subsection (1) must state that the applicant may ask for a review under Part 5.

New Brunswick deals with this issue in its *Right to Information and Protection of Privacy Act* (RIPPA) as follows:

> **Application deemed abandoned**
> **12**(1) If the head of the public body sends to the applicant a request for clarification in writing or a request in writing that the applicant shall pay or agree to pay fees for access to a record and the applicant does not respond to the request within 30 days after receiving the request, the request for access to a record shall be deemed abandoned.
>
> (2) If the request is deemed abandoned under subsection (1), the head shall notify the applicant in writing of his or her right to file a complaint with the Commissioner with respect to the abandonment.

Proposal

It is proposed that FOIP and LA FOIP be amended to have a section similar to Alberta with wording such as the following:

> **XX** (1) Where the head of a government institution (local authority) contacts an applicant in writing respecting the applicant's request, including:
>
> (a) seeking further information from the applicant that is necessary to process the request, or

(b) requesting the applicant to pay a fee or to agree to pay a fee, and the applicant fails to respond to the head of the government institution (local authority), as requested by the head, within 30 days after being contacted, the head of the government institution (local authority) may, by notice in writing to the applicant, declare the request abandoned.

(2) A notice under subsection (1) must state that the applicant may ask for a review by the commissioner.

19. Publicly Available Information

FOIP restricts government institutions from collecting, using or disclosing personal information but in many instances that personal information is publicly available through various public sources. In order to clarify when a government institution can obtain or use publicly available information, it is proposed we consider legislation to clarify the point.

British Columbia's *Personal Information Protection Act* (PIPA) provides as follows:

Collection of personal information without consent
12 (1) An organization may collect personal information about an individual without consent or from a source other than the individual, if

...

(d) the personal information is collected by observation at a performance, a sports meet or a similar event

(i) at which the individual voluntarily appears, and

(ii) that is open to the public,

(e) the personal information is available to the public from a source prescribed for the purposes of this paragraph,

…

Use of personal information without consent
15 (1) An organization may use personal information about an individual without the consent of the individual, if

...

(d) the personal information is collected by observation at a performance, a sports meet or a similar event

(i) at which the individual voluntarily appears, and

(ii) that is open to the public,

(e) the personal information is available to the public from a source prescribed for the purposes of this paragraph,

…

Disclosure of personal information without consent

18 (1) An organization may only disclose personal information about an individual without the consent of the individual, if

...

(d) the personal information is collected by observation at a performance, a sports meet or a similar event

(i) at which the individual voluntarily appears, and

(ii) that is open to the public,

(e) the personal information is available to the public from a source prescribed for the purposes of this paragraph,

Canada's PIPEDA provides as follows:

7. (1) For the purpose of clause 4.3 of Schedule 1, and despite the note that accompanies that clause, an organization may collect personal information without the knowledge or consent of the individual only if

...

(d) the information is publicly available and is specified by the regulations;

7. (2) For the purpose of clause 4.3 of Schedule 1, and despite the note that accompanies that clause, an organization may, without the knowledge or consent of the individual use personal information only if

...

(c.1) it is publicly available and is specified by the regulations;

7. (3) For the purpose of clause 4.3 of Schedule 1, and despite the note that accompanies that clause, an organization may disclose personal information without the knowledge or consent of the individual only if the disclosure is

...

(h.1) of information that is publicly available and is specified by the regulations;

Alberta's *Personal Information Protection Act* (PIPA) provides as follows:

Collection without consent

14 An organization may collect personal information about an individual without the consent of that individual but only if one or more of the following are applicable:

...

(e) the information is publicly available as prescribed or otherwise determined by the regulations;

Use without consent

17 An organization may use personal information about an individual without the consent of the individual but only if one or more of the following are applicable:

...

(e) the information is publicly available as prescribed or otherwise determined by the regulations;

Disclosure without consent
20 An organization may disclose personal information about an individual without the consent of the individual but only if one or more of the following are applicable:

...

(j) the information is publicly available as prescribed or otherwise determined by the regulations;

Proposal

It is proposed that a new section be added to FOIP and LA FOIP similar to that in Alberta. The proposed section might read as follows:

Collection without consent
XX A government institution (local authority) may collect, use or disclose personal information about an individual, without the consent of that individual, if the information is publicly available as prescribed in the regulations.

PART III
AMENDMENTS TO ASSIST THE COMMISSIONER

20. Grounds to Refuse to do a Review

Presently, we have section 50 in FOIP that focuses on not conducting a review if requests are frivolous, vexatious, not made in good faith or involves a trivial matter. Section 39 of LA FOIP has similar wording. HIPA is broader as follows:

Review or refusal to review
43(2) The commissioner may refuse to conduct a review or may discontinue a review if, in the opinion of the commissioner, the application for review:

(a) is frivolous or vexatious;

(b) is not made in good faith;

(c) concerns a trivial matter;

(d) does not affect the applicant personally;

(e) concerns a trustee that has an internal review process that the applicant has not used;

(f) concerns a professional who is governed by a health professional body or prescribed professional body mentioned in clause 27(4)(h) that regulates its members pursuant to an Act, and the applicant has not used a complaints procedure available through the professional body; or

(g) is normally considered pursuant to another Act that provides a review or other mechanism to challenge a trustee's decision with respect to the access to or collection, amendment, use or disclosure of personal health information, and the applicant has not used that review or mechanism.

Ontario's PHIPA provides:

No review
57(4) The Commissioner may decide not to review the subject-matter of the complaint for whatever reason the Commissioner considers proper, including if satisfied that,

(a) the person about which the complaint is made has responded adequately to the complaint;

PIPEDA provides as follows:

Discontinuance of Investigation
12.2(1) The Commissioner may discontinue the investigation of a complaint if the Commissioner is of the opinion that

(a) there is insufficient evidence to pursue the investigation;

(b) the complaint is trivial, frivolous or vexatious or is made in bad faith;

(c) the organization has provided a fair and reasonable response to the complaint;

(d) the matter is already the object of an ongoing investigation under this Part;

(e) the matter has already been the subject of a report by the Commissioner;

(f) any of the circumstances mentioned in paragraph 12(1)(a), (b) or (c) apply; or

(g) the matter is being or has already been addressed under a procedure referred to in paragraph 12(1)(a) or (b).

Proposal

It is proposed that section 50 in FOIP (section 39 LA FOIP) be amended to include the additional grounds referred to in HIPA, Ontario's legislation PHIPA and in the federal PIPEDA. It is proposed as follows:

50(2) The commissioner may refuse to conduct a review or investigation or may discontinue a review if, in the opinion of the commissioner, the application for review or investigation:

(a) is frivolous, vexatious or not made in good faith;

(b) does not affect the applicant personally;

(c) the applicant has failed to respond to the requests of the commissioner;

(d) the commissioner has determined the applicant's motives are to harass the government institution (local authority);

(e) the government institution (local authority) has responded adequately to the complaint;

(f) concerns a government institution (local authority) that has an internal review process that the applicant has not used;

(g) concerns a professional who is governed by a professional body or prescribed professional body that regulates its members pursuant to an Act, and the applicant has not used a complaints procedure available through the professional body; or

(h) is normally considered pursuant to another Act that provides a review or other mechanism to challenge a government institution (local authority)'s decision with respect to the access to or collection, amendment, use or disclosure of information, and the applicant has not used that review or mechanism;

(i) there is insufficient evidence to purse the review or investigation;

(j) the matter has already been the subject of a report by the commissioner.

21. Production of Documents

Presently the Commissioner can request production of documents but the head is not obliged to provide them within any specific time. As there is a need to speed up reviews or investigations, it would be helpful to require the head to produce the documents within 20 days unless the request involves a large amount of documents when more time should be allowed.

Newfoundland's ATIPPA provides:

> **Production of documents**
> **52**(1) the commissioner has the powers, privileges and immunities that are or may be conferred on a commissioner under the *Public Inquiries Act, 2006*.
> …
> (4) The head of a public body shall produce to the commissioner a record or a copy of a record required under this section within 14 days notwithstanding.

Proposal

It is proposed that section 54 of FOIP (section 43 LA FOIP) be amended to require the head to provide the Commissioner with the requested documents within 20 days. Wording might be as follows:

> **54**(1) Notwithstanding any other Act or any privilege that is available at law, the commissioner may, in a review:
>
> (a) require to be produced and examine within 20 days, any record that is in the possession or under the control of a government institution; and

22. Notice of Intention to Review

Section 51 of FOIP provides as follows:

> **Notice of intention to review**
> **51** Not less than 30 days before commencing a review, the commissioner shall inform the head of:
>
> (a) the commissioner's intention to conduct the review; and

The following is a provision presently found in the federal *Privacy Act*:

> **Notice of intention to investigate**
> **31** Before commencing an investigation of a complaint under this Act, the Privacy Commissioner shall notify the head of the government institution concerned of the intention to carry out the investigation and shall inform the head of the institution of the substance of the complaint.

In Ontario's FOIP, it provides:

> **Notice of intention for appeal**
> **50(3)** Upon receiving a notice of appeal, the Commissioner shall inform the head of the institution concerned of the notice of appeal and may also inform any other institution or person with an interest in the appeal, including an institution within the meaning of the *Municipal Freedom of Information and Protection of Privacy Act*, of the notice of appeal.

Proposal

It is proposed that section 51 of FOIP (section 40 LA FOIP) be amended as follows:

> **51** Upon commencement of a review or an investigation, the commissioner shall inform the head, the applicant and any third parties of:
>
> (a) the review or investigation; and
>
> (b) the substance of the review or investigation.

23. Determine Own Procedures

Presently FOIP and LA FOIP are silent on the issue of establishing procedures for reviews or investigations. The following is a provision in the federal *Privacy Act*:

> **Regulation of procedure**
> **32** Subject to this Act, the Commissioner may determine the procedure to be followed in the performance of any duty or function of the Commissioner under this Act.

The Ombudsman's Act, 2012 in Saskatchewan provides as follows:

> **Rules for guidance**
> **33**(1) On its own initiative or on the recommendation of the Lieutenant Governor in Council, the Legislative Assembly may make rules to guide the Ombudsman in the exercise of the Ombudsman's powers, and the performance of the Ombudsman's duties, pursuant to this Act.
>
> (2) Subject to this Act and any rules made pursuant to subsection (1), the Ombudsman may determine the procedure and the procedure for the members of the Ombudsman's staff in the exercise of their powers, and the performance of their duties, pursuant to this Act.

Proposal

It is proposed that a section be introduced into FOIP and LA FOIP to provide the Commissioner with similar procedure making abilities as provided in the federal Act. The section might provide as follows:

> **XX** Subject to this Act, the Commissioner may determine the procedure to be followed in the performance of any duty or function of the Commissioner under this Act.

24. Cross-jurisdictional Investigations

As we live in a more global world, personal information travels across borders much more frequently. Free trade and interprovincial trade increase the likelihood of information flowing across borders. Online shopping increases the flow of information across borders. Social media increases the flow. From time to time, it may be necessary for communication in neighboring provinces to do a joint review or investigation. Alberta and Saskatchewan have Lloydminster which is right on the border. Public bodies in that area may receive personal information from both Alberta and Saskatchewan public bodies.

Alberta's HIA provides:

> **General powers of Commissioner**
> **84**(1) In addition to the Commissioner's powers and duties under Divisions 1 and 2 with respect to reviews, the Commissioner is generally responsible for monitoring how this Act is administered to ensure its purposes are achieved, and may
>
> …

(j) exchange information with an extra-provincial commissioner and enter into information sharing and other agreements with extra-provincial commissioners for the purpose of co-ordinating activities and handling complaints involving 2 or more jurisdictions.

(2) For the purposes of subsection (1)(j), "extra-provincial commissioner" means a person who, in respect of Canada or in respect of another province or territory of Canada, has duties, powers and functions similar to those of the Commissioner.

Ontario's PHIPA includes the following but is not as clear:

General powers
66. The Commissioner may,

…

(e) assist in investigations and similar procedures conducted by a person who performs similar functions to the Commissioner under the laws of Canada, except that in providing assistance, the Commissioner shall not use or disclose information collected by or for the Commissioner under this Act;

Proposal

It is proposed that FOIP and LA FOIP have a section similar to Alberta as follows:

XX(1) In addition to the Commissioner's powers and duties in this Act, the Commissioner is generally responsible for monitoring how this Act is administered to ensure its purposes are achieved, and may exchange information with an extra-provincial commissioner and enter into information sharing and other agreements with extra-provincial commissioners for the purpose of co-ordinating activities and handling complaints involving two or more jurisdictions.

(2) For the purposes of subsection (1), "extra-provincial commissioner" means a person who, in respect of Canada or in respect of another province or territory of Canada, has duties, powers and functions similar to those of the Commissioner.

25. Conflict of Interest of Commissioner

In cases of conflict of interest of the Commissioner, Saskatchewan has no provision to allow delegation to a staff member. A provision such as the one from PEI's FOIPP would assist in these situations:

Delegation
58(1) The Commissioner may delegate to any person any function of the Commissioner under this Act, except the power to delegate under this section.

(2) A delegation under subsection (1) shall be in writing and may contain any conditions or restrictions the Commissioner considers appropriate.

Alberta's FOIP has specific conflict of interest language as follows:

> **Review where Commissioner in conflict**
> **78**(1) This section applies where the Commissioner is asked under section 65(1), (2), (3) or (4) to review a decision, act or failure to act of a head of a public body and the Commissioner had been a member, employee or head of that public body or, in the Commissioner's opinion, the Commissioner has a conflict with respect to that public body.

Proposal

It is proposed that FOIP and LA FOIP have a section which would allow the Commissioner to delegate in situations where he or she has a conflict of interest such as the following:

> **XX** (1) The Commissioner may delegate to any person any function of the Commissioner under this Act, where in his or her opinion, has a conflict of interest.
>
> (2) A delegation under subsection (1) shall be in writing and may contain any conditions or restrictions the Commissioner considers appropriate.

26. Issuing Reports

Presently, FOIP and LA FOIP only require a report to be issued in the case of a review. An example of this is in subsection 55(1) of FOIP:

> **Commissioner to report**
> **55**(1) On completing a review, the commissioner shall:
>
> …
>
> (d) prepare a written report setting out the commissioner's recommendations with respect to the matter and the reasons for those recommendations; and

Sometimes during the review the government institution releases the information, or the Applicant cannot be found or there are other reasons that the report would be issued with no recommendations. The Commissioner is attempting to be more collaborative and it is hoped matters can be resolved at an earlier stage in the process. The use of the word "shall" takes away the Commissioner's flexibility.

Proposal

It is proposed that subsection 55(1) of FOIP [subsection 44(1) LA FOIP] be amended by replacing "shall" with "may".

> **XX**(1) On completing a review or investigation, the commissioner may:
>
> …
>
> (e) prepare a written report setting out the commissioner's recommendations with respect to the matter and the reasons for those recommendations; and

27. Response by the Head

Subsection 56(1) of FOIP (subsection 45(1) of LA FOIP) requires a head to respond to the Commissioner's report in 30 days. In today's world that is just too long. In other sections of this report, it has been proposed that timelines be shortened, so as to speed up the process.

Proposal

It is proposed that the 30 days in subsection 56(1) of FOIP (subsection 45(1) of LA FOIP) be reduced to 20 days.

28. Appeals

Presently FOIP and LA FOIP do not allow the Commissioner to participate in appeals made to the Court of Queen's Bench. It is proposed that section 57 of FOIP (section 46 LA FOIP) be amended to allow the Commissioner to make representations to or intervene in an appeal to the Court of Queen's Bench.

Proposal

57(1) Within 30 days after receiving a decision of the head pursuant to section 56 that access is granted or refused, an applicant or a third party may appeal that decision to the court.

(2) A head who has refused an application for access to a record or part of a record shall, immediately on receipt of a notice of appeal by an applicant give written notice of the appeal to any third party that the head:

(a) has notified pursuant to subsection 34(1) or

(b) would have notified pursuant to subsection 34(1) if the head had intended to give access to the record or part of the record.

(3) A head who has granted an application for access to a record or part of a record shall, immediately on receipt of a notice of appeal by a third party, give written notice of the appeal to the applicant.

(4) A third party who has been given notice of an appeal pursuant to subsection (2) or an applicant who has been given notice of an appeal pursuant to subsection (3) may appear as a party to the appeal.

(5) The commissioner may intervene in an appeal and make representations to the court.

29. Offences Under the Act

Presently FOIP provides that the Commissioner (and his/her staff) is non-compellable (section 47) and that the Commissioner shall conduct every review in private (section 53 of FOIP and section 42 of LA FOIP). In cases where there is a prosecution of an offence under the Act this can hinder the Commissioner's ability (and his/her staff) to be called as a witness and/or to produce relevant documentation during a prosecution. The office notes that this ability is provided for in section 45 of British Columbia's FOIP which provides as follows:

> **45**(1) A statement made or an answer given by a person during an investigation or inquiry by the commissioner is inadmissible in evidence in court or in any other proceeding, except
>
> (a) in a prosecution for perjury in respect of sworn testimony,
>
> (b) in a prosecution for an offence under this Act, or
>
> (c) in an application for judicial review or an appeal from a decision with respect to that application.
>
> (2) Subsection (1) applies also in respect of evidence of the existence of proceedings conducted before the commissioner.

Proposal

It is proposed that section 47 of FOIP be amended to allow the Commissioner (and his/her staff) to be a witness and/or produce relevant documentation in the event of a prosecution only. The amended section might read as follows:

> **47**(1) The commissioner is not compellable to give evidence in a court or in a proceeding of a judicial nature concerning any information that comes to the knowledge of the commissioner in the exercise of the powers, performance of the duties or carrying out of the functions of the commissioner pursuant to this Act.
>
> (2) Subsection (1) applies, with any necessary modification, to the staff of the commissioner.
>
> (3) In the event of a prosecution of an offence under this Act, the commissioner or the staff of the commissioner may be a witness or produce documents relevant to the prosecution.

It is noted that LA FOIP does not have a provision similar to section 47 of FOIP. Therefore, it is also proposed that a section 47 of FOIP be added to LA FOIP.

30. Offence Provisions in FOIP and LA FOIP

Presently in FOIP and LA FOIP, the offence provision only includes a fine of $1,000 and imprisonment of up to three months. The present wording in FOIP is as follows:

Offence

68(1) Every person who knowingly collects, uses or discloses personal information in contravention of this Act or the regulations is guilty of an offence and liable on summary conviction to a fine of not more than $1,000, to imprisonment for not more than three months or to both fine and imprisonment.

LA FOIP's section 56 is similarly worded.

HIPA includes the following language:

Offences

64(1) No person shall:

(a) knowingly contravene any provision of this Act or the regulations;

(b) without lawful justification or excuse, wilfully obstruct, hinder or resist the commissioner or any other person in the exercise of the powers, performance of the duties or the carrying out of the functions of the commissioner or other person pursuant to this Act;

(c) without lawful justification or excuse, refuse or wilfully fail to comply with any lawful requirement of the commissioner or any other person pursuant to this Act;

(d) wilfully make any false statement to, or mislead or attempt to mislead, the commissioner or any other person in the exercise of the powers, performance of the duties or carrying out of the functions of the commissioner or other person pursuant to this Act;

(e) wilfully destroy any record that is governed by this Act with the intent to evade a request for access to the record; or

(f) obtain another person's personal health information by falsely representing that he or she is entitled to the information.

(2) Every person who contravenes subsection (1) is guilty of an offence and is liable on summary conviction:

(a) in the case of an individual, to a fine of not more than $50,000, to imprisonment for not more than one year or to both; and

(b) in the case of a corporation, to a fine of not more than $500,000.

(3) Every director, officer or agent of a corporation who directed, authorized, assented to, acquiesced in or participated in an act or omission of the corporation that would constitute an offence by the corporation is guilty of that offence, and is liable on summary conviction to a fine of not more than $50,000, to imprisonment for not more than one year or to both, whether or not the corporation has been prosecuted or convicted.

(4) No prosecution shall be commenced pursuant to this section except with the express consent of the Attorney General for Saskatchewan.

(5) No prosecution shall be commenced pursuant to this section after the expiration of two years after the date of the discovery of the alleged offence.

Public sector privacy legislation in Alberta and New Brunswick prescribes a statutory time limit on the commencement of prosecutions at two years. The only difference between the two is the commencement of the time period. In Alberta the time limit begins from the date of the commission of the offence. In New Brunswick the time limit begins from the date of discovery.

Proposal

It is proposed that FOIP and LA FOIP be amended to parallel HIPA's section 64 with increased maximum fines, months of imprisonment and a two year limitation on prosecution.

It is also proposed that purposefully destroying a record is an offense. The following language is from Newfoundland's ATIPPA*:*

Offence

72. A person who wilfully

…

(d) destroys a record or erases information in a record that is subject to this Act with the intent to evade a request for access to records,

is guilty of an offence and liable, on summary conviction, to a fine of not more than $5,000 or to imprisonment for a term not exceeding 6 months, or to both.

Snooping by employees into personal information has become an issue in our society. The Minister of Health has recently introduced amendments to HIPA to create stronger offences for employees caught snooping. The proposed amendments are as follows:

64(3.1) An individual who is an employee of or in the service of a trustee or information management service provider and who knowingly discloses or directs another person to disclose personal health information in circumstances that would constitute an offence by the trustee or information management service provider pursuant to this Act is guilty of an offence and is liable on summary conviction to a fine of not more than $50,000, to imprisonment for not more than one year or to both, whether or not the trustee or information management service provider has been prosecuted or convicted.

(3.2) An individual who is an employee of or in the service of a trustee and who wilfully accesses or uses or directs another person to access or use personal health information that is not reasonably required by that individual to carry out a purpose authorized pursuant to this Act is guilty of an offence and is liable on summary conviction to a fine of not more than $50,000, to imprisonment for not more than one year or to both, whether or not the trustee has been prosecuted or convicted.

It is assumed these provisions will pass in the spring of 2015. It is most helpful when provisions are similar in FOIP, LA FOIP and HIPA. It is proposed there be additional offence provisions in FOIP and LA FOIP as follows:

> **Offence**
> **68.1**(1) An individual who is an employee of or in the service of a government institution (local authority) or information management service provider, contractor or consultant and who knowingly discloses or directs another person to disclose personal information in circumstances that would constitute an offence by the government institution (local authority) or information management service provider, contractor or consultant pursuant to this Act is guilty of an offence and is liable on summary conviction to a fine of not more than $50,000, to imprisonment for not more than one year or to both, whether or not the government institution (local authority) or information management service provider, contractor or consultant has been prosecuted or convicted.
>
> (2) An individual who is an employee of or in the service of a government institution (local authority) and who wilfully accesses or uses or directs another person to access or use personal information that is not reasonably required by that individual to carry out a purpose authorized pursuant to this Act is guilty of an offence and is liable on summary conviction to a fine of not more than $50,000, to imprisonment for not more than one year or to both, whether or not the government institution (local authority) has been prosecuted or convicted.

Further, Ontario has introduced an amendment to PHIPA that makes it an offense to destroy documents which have been created. Ontario's proposed provision provides as follows:

> **61**(1)
> ...
> (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;

FOIP and LA FOIP do not have such an offense. It is proposed that a provision similar to Ontario's be added in FOIP and LA FOIP.

31. Privacy Impact Assessment

Government institutions and local authorities deal with a lot of personal information. They introduce new programs and develop new computer systems. When these major changes occur, it is only reasonable that they step back and do a privacy impact assessment. This fits with the concept that entities should manage risks. Inappropriate release of personal information is a risk. Doing an assessment at the beginning reduces the risk of breaches.

A *Privacy Impact Assessment* (PIA) is a diagnostic tool designed to help organizations assess their compliance with the privacy requirements of Saskatchewan legislation. No legal obligation exists presently for public bodies in Saskatchewan to complete these, nor is there a requirement for providing those to the Commissioner for comment. In order to ensure that privacy protective

practices are embedded in program design at the beginning, I believe PIAs should be mandatory in some cases. It is always more difficult, time consuming and costly to try to make changes after the fact if missed in the design and implementation phases.

New Brunswick's *Personal Health Information Privacy and Access Act* includes the following provision on requiring PIAs:

> **56**(1) A custodian that is a public body or any other custodian prescribed by regulation shall conduct a privacy impact assessment in the following situations:
>
> (a) for the new collection, use or disclosure of personal health information or any change to the collection, use or disclosure of personal health information;
>
> (a.1) for the creation of an integrated service, program or activity or a modification to an integrated service, program or activity;
>
> (b) for the creation of a personal health information system or personal health information communication technology or a modification to a personal health information system or personal health information communication technology;
>
> (c) subject to section 57, if a custodian performs data matching with personal health information or with any personal health information held by another custodian or another person.
>
> **56**(1.1) Paragraph (1)(a) does not apply to the collection, use or disclosure of personal health information if the collection, use or disclosure is necessary for the delivery of an existing integrated service, program or activity.
>
> **56**(2) A privacy impact assessment shall describe, in the form and manner as may be prescribed by regulation, how the proposed administrative practices and information systems relating to the collection, use and disclosure of individually identifying health information may affect the privacy of the individual to whom the information relates.

Alberta's HIA includes the following provision on PIAs:

> **Duty to prepare privacy impact assessment**
> 64(1) Each government institution (local authority) must prepare a privacy impact assessment that describes how proposed administrative practices and information systems relating to the collection, use and disclosure of individually identifying personal information may affect the privacy of the individual who is the subject of the information.
>
> (2) The custodian must submit the privacy impact assessment to the Commissioner for review and comment before implementing any proposed new practice or system described in subsection (1) or any proposed change to existing practices and systems described in subsection (1).

Proposal

It is proposed wording similar to Alberta's be included in FOIP and LA FOIP which might provide as follows:

> **XX**(1) A government institution (local authority) must prepare a privacy impact assessment that describes how proposed administrative practices and information systems relating to the collection, use and disclosure of individually identifying personal information may affect the privacy of the individual who is the subject of the information.
>
> (2) The government institution (local authority) must submit the privacy impact assessment to the Commissioner for review and comment before implementing any proposed new practice or system described in subsection (1) or any proposed change to existing practices and systems described in subsection (1).

PART IV
GENERAL

32. Statutes Subject to FOIP and LA FOIP

Presently FOIP provides as follows:

> **23**(3) Subsection (1) does not apply to:
>
> (a) *The Adoption Act, 1998;*
>
> (b) section 27 of *The Archives Act, 2004*;
>
> (c) section 74 of *The Child and Family Services Act*;
>
> (d) Section 7 of *The Criminal Injuries Compensation Act*;
>
> (e) section 12 of *The Enforcement of Maintenance Orders Act*;
>
> (e.1) *The Health Information Protection Act*;
>
> (f) section 38 of *The Mental Health Services Act*;
>
> (f.1) section 91.1 of *The Police Act, 1990*;
>
> (g) section 13 of *The Proceedings against the Crown Act*;
>
> (h) sections 15 and 84 of *The Securities Act, 1988*;
>
> (h.1) section 61 of *The Trust and Loan Corporations Act, 1997*;

(i) section 283 of *The Traffic Safety Act*;

(i.1) subsection 97(4) of *The Traffic Safety Act*;

(j) Part VIII of *The Vital Statistics Act, 2009*;

(j.1) section 12 of *The Vital Statistics Administration Transfer Act*;

(k) sections 172 to 174 of *The Workers Compensation Act, 2013*;

(l) any prescribed Act or prescribed provisions of an Act; or

(m) any prescribed regulation or prescribed provisions of a regulation; and the provisions mentioned in clauses (a) to (m) shall prevail.

Section 12 of the FOIP Regulations provide:

Confidentiality provisions in other enactments
12 For the purposes of clause 23(3)(l) of the Act, the following provisions are prescribed as provisions to which subsection 23(1) of the Act does not apply:

(a) section 178 of *The Election Act, 1996*;

(b) section 75 of *The Vital Statistics Act, 2009*;

(c) section 43 of *The Occupational Health and Safety Act, 1993*;

(d) Part III of *The Revenue and Financial Services Act*;

(e) all of *The Income Tax Act* and *The Income Tax Act, 2000;*

(f) section 32 of *The Safer Communities and Neighbourhoods Act;*

(g) section 14 of *The Enforcement of Maintenance Orders Act, 1997*;

(h) section 415 of *The Credit Union Act, 1998*;

(i) section 85 of *The Real Estate Act*;

(j) section 10.1 of *The Saskatchewan Insurance Act*

(k) section 12 of *The Vital Statistics Administration Transfer Act;*

(l) section 61 of *The Mortgage Brokerages and Mortgage Administrators Act*;

(m) section 61 of *The Payday Loans Act.*

Proposal

FOIP is 23 years old and as time passes the government has opted to add sections of Acts that are not subject to FOIP. The list has become rather long and consists of some 26 exceptions. In reviewing FOIP, I would propose a careful review of the list of exceptions.

In that review, I would suggest that where an Act or a part of an Act is exempted, consideration be given to exempt only specific sections that restrict or prohibit access.

33. Five Year Review

Many access and privacy laws in Canada contain a statutory requirement for a review by a legislative committee after a fixed period of three or five years. An example would be the provision in Alberta's FOIP that came into force in 1995 and has been revised in two subsequent amendment packages that resulted from all-party reviews in 1998 and 2001.

FOIP was introduced in 1992 and LA FOIP was introduced in 1993. Neither of those Acts has been periodically reviewed or updated. To ensure that these Acts are regularly revisited in terms of amendments, it is proposed that review provisions be added to FOIP and LA FOIP.

Newfoundland's ATIPPA provides:

> **Review**
> **74.** After the expiration of not more than 5 years after the coming into force of this Act or part of it and every 5 years thereafter, the minister responsible for this Act shall refer it to a committee for the purpose of undertaking a comprehensive review of the provisions and operation of this Act or part of it.

What follows is a brief summary of relevant legislative review activity in other jurisdictions:

CANADIAN FEDERAL *ACCESS TO INFORMATION ACT*

The federal *Access to Information Act* was enacted in 1983. In March 1987, the Standing Committee on Justice and Solicitor General released its review of the Act, *Open and Shut: Enhancing the Right to Know and the Right to Privacy*. Later the same year the government released its response, *Access and Privacy: The Steps Ahead*. A federal Task Force reported on June 12, 2002 and made 139 recommendations for legislative change in its report *Access to Information: Making it Work for Canadians*. The government then released *A Comprehensive Framework for Access to Information Reform: A Discussion Paper*. On November 15, 2005, the Honourable Gérard V. La Forest, Special Advisor to the Minister of Justice tabled his report - *The Offices of the Information and Privacy Commissioners: The Merger and Related Issues*. In April 2006, the federal government produced *Strengthening the Access to Information Act: A Discussion of Ideas Intrinsic to the Reform of the Access to Information Act*. Part of the *Federal Accountability Act* addressed changes to the *Access to Information Act.*

CANADIAN FEDERAL *PRIVACY ACT*

The March 1987 Report from the Standing Committee of Justice and Solicitor General discussed above, also reviewed the *Privacy Act*. That was followed later the same year

by the government's response: *Access and Privacy: The Steps Ahead*. In June 2006, the document *Government Accountability for Personal Information – Reforming the Privacy Act* was issued by the Privacy Commissioner of Canada, and an Addendum to that document was issued in April 2008. The Standing Committee on Access to Information, Privacy and Ethics is reviewing the *Privacy Act* and is currently taking submissions and interviewing witnesses.

ONTARIO

The Ontario PHIPA came into force in 1988 and included a statutory requirement to "*on or before the 1st day of January, 1991, undertake a comprehensive review of this Act and shall, within one year after beginning that review, make recommendations to the Legislative Assembly regarding amendments to this Act*." The initial review resulted in a Report of the Standing Committee on the Legislative Assembly in January 1991 and included 81 different recommendations for amendment. There was a subsequent review of the municipal FOIP Act by the Standing Committee on Legislative Assembly in 1994 that included 84 different recommendations for amendment.

NOVA SCOTIA

In 1977, Nova Scotia became the first province to pass access to information legislation. The legislation was replaced by a new statute in 1994 when the new *Freedom of Information and Protection of Privacy Act* (FOIPOP) came into effect. In 1996, an advisory committee was set up in accordance with the Act to review the legislation, and issued a report with 64 recommendations. Some of these were addressed by the legislature in 1998 and others in 1999.

QUEBEC

Legislation in Quebec created the Commission d'accès à l'information (CAI) in 1982. Substantial amendments were made by Bill 86 introduced in the National Assembly in 2005.

MANITOBA

When *The Freedom of Information and Protection of Privacy Act* (FIPPA) came into force it included a requirement for a 5 year review by the Legislative Assembly. A similar provision appeared in *The Personal Health Information Act* (PHIA) when enacted in 1997. There was a public consultation in 2004 and an amending bill is currently before the Manitoba Assembly.

ALBERTA

There were two major statutorily mandated reviews of the FOIP Act by all-party committees of the Legislative Assembly in 1998 and 2001. Both reports from these reviews resulted in an amendment of the FOIP Act in 1999. The *Health Information Act* that came into force in 2001 was reviewed by an all-party committee in 2004 that resulted in a number of amendments. A further review is currently underway.

BRITISH COLUMBIA

There have been two reports of statutorily mandated reviews of the *Freedom of Information and Protection of Privacy Act* (FOIPPA) by all-party committees of the Legislative Assembly. The first was in 1999 and the second in 2004. The next review must be undertaken starting next year.

Amendments have been made to FOIPPA stemming from both reviews, although the latest report's recommendations are in large measure still under consideration.

Since FOIPPA came into force in 1993 there have been many other amendments, including the USA Patriot Act changes. From this session, Bill 13 awaits Royal Assent. Its amendments stem from the 2004 review.

Proposal

It is proposed to introduce a new section in FOIP and LA FOIP that would provide for a periodic review of both statutes. The wording might be as follows:

> **XX** After five years, after the coming into force of this Act and every five years thereafter, the minister responsible for this Act shall refer it to a committee for the purpose of undertaking a comprehensive review of the provisions and operations of this Act.

34. Saskatchewan's Private Sector Employees

Should Saskatchewan adopt a law similar to British Columbia's *Personal Information Protection Act* (PIPA) and Alberta's *Personal Information Protection Act* (PIPA) to displace PIPEDA and thereby extend privacy protection to all private sector employees?

Proposal

It is proposed that legislation be introduced to provide protection to employees in the private sector similar to the protections employees have in the public sector.

35. Consolidation of FOIP/LA FOIP

FOIP and LA FOIP have many similar provisions but the similar provisions have different section numbers. Citizens can be confused as to which Act applies.

Proposal

Since the provisions are so similar, it is proposed that FOIP and LA FOIP be merged into one Act that deals with all "public bodies". Although this is an important step and should be taken, if it causes delay or too much opposition, it should not be pursued. The other requested amendments are important enough that they should proceed as quickly as possible.

All other provinces have one statute except Ontario who has two.